Return to Menu

Part No. P0937663 02

Business Communications Manager 2.5

IP Telephony Configuration Guide

NORTEL NETWORKS™

Copyright © 2001 Nortel Networks

All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Contents

Preface 13

Before you begin 13
Symbols used in this guide 14
Text conventions 14
Acronyms 15
Related publications 17
How to get help 18

Chapter 1
Introduction 19

IP telephones and VoIP trunks 19
IP telephones 20
VoIP trunks 20
The IP telephony network 20
Business Communications Manager 21
M1-ITG 22
Telephones 22
Traditional telephones 22
IP telephones 22
H.323 terminals 22
Gatekeeper 22
IP Network 22
WAN 23
LAN 23
Public Switched Telephone Network 23
Key IP Telephony Concepts 23
Codecs 23
Jitter Buffer 24
QoS routing 24

Chapter 2
Prerequisites checklist 27

Network diagram 27
Network devices 27
Network assessment 28
Resource Assessment 28
Keycodes 29
Business Communications Manager System Configuration 29
IP Telephones 30

Chapter 3
Installing IP Telephones 31

Preparing your Business Communications Manager for IP telephone registration . . . 31
Choosing a codec 33
Choosing a Jitter Buffer 33
Installing and Configuring i2004 Internet Telephones 34
Before Installing 34
Using a 3-port switch 34
Connecting the i2004 Internet telephone 34
Configuring the i2004 telephone 35
Troubleshooting an IP telephone 36
Configuring DHCP 38
Modifying settings for Nortel IP telephones 40
Download Firmware to an i200X telephone 43
Deregistering DNs for online IP telephones 44
Deregistering offline DNs 45
Moving IP telephones 46
Configuring the i2050 Software Phone 46
H.323 devices 47
Adding H.323 devices to the system 48

Chapter 4
VoIP Trunk Configuration 51

Installing keycodes 51
Setting the Published IP Address 51
Determining the published IP address 52
Configuring media parameters 53
Configuring codecs 54
Setting Silence Compression 54
Setting Jitter Buffers 55
Outgoing call configuration 56
Putting VoIP lines into a line pool 57
Configuring the Access code for the Line Pool 58
Configuring DNs to access the VoIP line pool 58
Configuring a remote gateway 59
Configuring PSTN fallback 60
Setting up a VoIP schedule 61
Configuring routes 63
Creating a destination code 65
Configuring digits 67
Activating the VoIP schedule 67

Turning on QoS monitor 68
Enabling PSTN fallback 70
Incoming call configuration 70
Assign a target line to the DN 70
Example configuration 71
On Business Communications Manager Ottawa 72
On Business Communications Manager Santa Clara 73
Making calls 74
Connecting an i200X telephone 75
Connecting an i200X telephone on the LAN 75
Configuring NetMeeting clients 75
Quality of Service Monitor 77
Quality of Service Status 77
Updating the QoS Monitor data 77
Port settings 77
Using firewalls 78
Port settings for legacy networks 79
Using a gatekeeper 80
The call signalling method 80
Alias names 80
Modifying the call signalling method 81
Gatekeeper call scenarios 82

Chapter 5
Typical applications 85

M1 to Business Communications Manager over IP trunks 85
MCDN functionality 86
Multiple Business Communications Manager systems across VoIP trunks 86
Multi-location chain with call center 87
Business Communications Manager to IP Telephones 89

Appendix A
Networking 91

Determining the bandwidth requirements 91
Determining WAN link resources 91
Link utilization 91
Network Engineering 92
Bandwidth Requirements on Half Duplex Links 93
Bandwidth Requirements on Full Duplex Links 94
LAN Engineering Examples 95
WAN engineering 96

Additional feature configuration 96
Setting Non-linear processing 96
Determining network loading caused by IP telephony traffic 96
Other intranet resource considerations 99
Implementing the network 99
LAN engineering 99
Getting the best results from your system 99
Further network analysis 99
Components of delay 99
Reduce link delay 100
Reducing hop count 100
Routing issues 102
Post-installation network measurements 102

Appendix B
Silence compression 103

Silence compression on Half Duplex Links 103
Silence compression on Full Duplex Links 105
Comfort Noise 108
. 108

Appendix C
Network Performance Utilities 109

Ping 109
Traceroute 109
Sniffer 109

Appendix D
Interoperability 111

Speech Path Setup Methods 112
Media Path Redirection 112
Gatekeeper 113
Asymmetrical Media Channel Negotiation 113
No feedback busy station 113
Symbol Telephones 114

Appendix E
Quality of Service 115

Setting QoS 115
Measuring Intranet QoS 116
Measuring end-to-end network delay 116
Measuring end-to-end packet loss 117

Recording routes 117
Adjusting ping measurements 118
Measurement procedure 118
Other measurement considerations 119
Implementing QoS in IP networks 120
Traffic mix 120
TCP traffic behavior 121
Business Communications Manager Router QoS Support 121
Network Quality of Service 121
Network Monitoring 122
Quality of Service parameters 122
Fallback to PSTN 123
Glossary 125
Index 127

Figures

Figure 1 Network diagram . . . 21
Figure 2 Set registration properties . . . 32
Figure 3 Global options . . . 38
Figure 4 DHCP summary . . . 39
Figure 5 DHCP range . . . 40
Figure 6 IP Terminal status . . . 41
Figure 7 Configuration menu . . . 42
Figure 8 Terminal status dialog . . . 42
Figure 9 IP Terminal Status . . . 43
Figure 10 IP Terminal Status . . . 44
Figure 11 Deregister Offline DN . . . 45
Figure 12 i2050 Communications server . . . 47
Figure 13 i2050 Switch type . . . 47
Figure 14 H.323 Terminal list . . . 48
Figure 15 H.323 Terminal list dialog . . . 49
Figure 16 Global IP settings . . . 52
Figure 17 Setting the Published IP address . . . 53
Figure 18 Media parameters . . . 54
Figure 19 Media Parameters . . . 55
Figure 20 Media parameters . . . 56
Figure 21 Trunk/Line data . . . 57
Figure 22 Line pool . . . 58
Figure 23 Remote gateway list . . . 59
Figure 24 Remote gateway dialog . . . 60
Figure 25 PSTN fallback diagram . . . 61
Figure 26 VoIP schedule . . . 62
Figure 27 VoIP Routing Service . . . 63
Figure 28 Route list . . . 64
Figure 29 Add route dialog . . . 64
Figure 30 Add route dialog . . . 65
Figure 31 Add destination code dialog . . . 65
Figure 32 Normal schedule . . . 66
Figure 33 VoIP schedule . . . 67
Figure 34 Remote Gateway list . . . 69
Figure 35 Remote Gateway dialog . . . 69
Figure 36 Example PSTN fallback . . . 71
Figure 37 NetMeeting options . . . 76
Figure 38 NetMeeting advanced options . . . 76
Figure 39 Port Ranges . . . 78
Figure 40 Port ranges dialog . . . 79

Figure 41 Local gateway IP interface 81
Figure 42 Business Communications Manager systems with a gatekeeper 82
Figure 43 M1 to Business Communications Manager network diagram 85
Figure 44 Multiple Business Communications Manager systems network diagram 87
Figure 45 M1 to Business Communications Manager network diagram 88
Figure 46 M1 to Business Communications Manager network diagram 89
Figure 47 Calculating network load with IP telephony traffic 97
Figure 48 One Call on a Half Duplex Link Without Silence compression 104
Figure 49 One Call on a Half Duplex Link With Silence compression 104
Figure 50 Two Calls on a Half Duplex Link With Silence compression 105
Figure 51 One Call on a Full Duplex Link Without Silence compression 106
Figure 52 One Call on a Full Duplex Link With Silence compression 107
Figure 53 Two Calls on a Full Duplex Link With Silence compression 108
Figure 54 Relationship between users and services 115

Tables

Table 1 Network diagram 27
Table 2 Network device checklist 28
Table 3 Network assessment 28
Table 4 Resource Assessment 29
Table 5 Keycodes 29
Table 6 Business Communications Manager system configuration 30
Table 7 IP telephones 30
Table 8 Settings for IP telephones 35
Table 9 QoS status 77
Table 10 Voice over IP Transmission Characteristics for unidirectional continuous media stream 93
Table 11 Bandwidth Requirements per BCM Gateway port for half-duplex links. . 94
Table 12 Bandwidth Requirements per BCM Gateway port for Full-duplex links. . 95
Table 13 Link capacity example 98
Table 14 Business Communications Manager 2.5 Product Interoperability Summary 111
Table 15 Engineering specifications 111
Table 16 Supported voice payload sizes 112
Table 17 Name comparison 113
Table 18 Quality of voice service 116
Table 19 Site pairs and routes 117
Table 20 Computed load of voice traffic per link 118
Table 21 Delay and error statistics 119

Preface

This guide describes IP Telephony functionality for the Business Communications Manager 2.5 system. This includes information on Nortel IP terminals such as the i2004 phone and the i2050 software phone, H.323 terminals and H.323 trunks.

Before you begin

This guide is intended for installers and managers of a Business Communications Manager 2.5 system. Prior knowledge of IP networks is required.

Before using this guide, you must install and configure a Business Communications Manager 2.5 system.

This guide assumes:

- You have planned the telephony and data requirements for your Business Communications Manager 2.5 system.
- The Business Communications Manager 2.5 is installed and initialized and the hardware is working. External lines and terminals and sets are connected to the appropriate media bay modules on the Business Communications Manager 2.5.
- Configuration of lines is complete.
- Operators have a working knowledge of the Windows operating system and graphical user interfaces.
- Operators who manage the data portion of the system are familiar with network management and applications.

Refer to Chapter 2, “Prerequisites checklist,” on page 27 for more information.

Symbols used in this guide

This guide uses these symbols to draw your attention to important information:

Caution: Caution Symbol
Alerts you to conditions where you can damage the equipment.

Danger: Electrical Shock Hazard Symbol
Alerts you to conditions where you can get an electrical shock.

Warning: Warning Symbol
Alerts you to conditions where you can cause the system to fail or work improperly.

Note:
Alerts you to important information.

Tip: Tip Symbol
Alerts you to additional information that can help you perform a task.

Text conventions

This guide uses these following text conventions:

angle brackets (< >)	Represent the text you enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is `ping <ip_address>`, you enter `ping 192.32.10.12`
`bold Courier text`	Represent command names, options and text that you need to enter. Example: Use the **`dinfo`** command. Example: Enter **`show ip`** {**`alerts`**|**`routes`**}.

italic text	Represents terms, book titles and variables in command syntax descriptions. If a variable is two or more words, the words are connected by an underscore. Example: The command syntax `show at <valid_route>`, `valid_route` is one variable and you substitute one value for it.
`plain Courier text`	Represents command syntax and system output, such as prompts and system messages. Example: `Set Trap Monitor Filters`

Acronyms

This guide uses the following acronyms:

ATM	Asynchronous Transfer Mode
BCM	Business Communications Manager
CIR	Committed Information Rate
DID	Direct Inward Dialing
DOD	Direct Outward Dialing
DIBTS	Digital In-Band Trunk Signalling
DSB	DIBTS Signalling Buffer
ITU	International Telecommunication Union
IXC	IntereXchange Carrier
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LATA	Local Access and Transport Area
LEC	Local Exchange Carrier
MOS	Mean Opinion Score
PCM	Pulse Code Modulation
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTP	Real-time Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol

UDP	User Datagram Protocol
UTPS	UNISTEM Terminal Proxy Server
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

Related publications

Documents referenced in the *Business Communications Manager 2.5 IP Telephony Configuration Guide*, include:

- Business Communications Manager 2.5 Installation and Maintenance Guide
- Business Communications Manager 2.5 Software Keycode Installation Guide
- Business Communications Manager 2.5 Telephone Features Guide

How to get help

Your local distributor can provide technical support for your Business Communications Manager system or have access to that information through a Technical Service Center (TSC).

If you require non-technical support, contact 1-800-4NORTEL (1-800-466-7835), choose option 3, Sales or Pre-Sales Support)

Chapter 1
Introduction

IP Telephony provides the flexibility, affordability and expandability of the Internet to the world of voice communications. Business Communications Manager for VoIP gives you several critical advantages:

- **Cost Savings.** IP networks can be significantly less expensive to operate and maintain than traditional networks. The simplified network infrastructure of an Internet Telephony solution cuts costs by connecting IP telephones over the LAN wiring system and eliminates the need for dual cabling. Internet Telephony can also eliminate toll charges on site-to-site calls via global four-digit dialing. And, by using the extra bandwidth on your WAN for IP Telephony, you leverage the untapped capabilities of your data infrastructure to maximize the return on your current network investment.
- **Portability and flexibility**. Employees can be more productive because they are no longer confined by geographic location. IP telephones work anywhere on the network, even over a remote connection. With Nortel Networks wireless e-mobility solutions, your phone, laptop, or scanner can work anywhere on the network where a Nortel Networks Access Point is installed. Network deployments and reconfigurations are simplified, and service can be extended to remote sites and home offices over cost-effective IP links.
- **Simplicity and consistency**. A common approach to service deployment allows further cost-savings from the use of common management tools, resource directories, flow-through provisioning, and a consistent approach to network security. As well, customers can centrally manage a host of multimedia services and business-building applications from a central point via a Web-based browser. The ability to network existing PBXs using IP can bring new benefits to your business. For example, the ability to consolidate voice mail onto a single system, or to fewer systems, making it easier for voice mail users to network.
- **Compatibility**. Internet Telephony is supported over a wide variety of transport technologies. A user can gain access to just about any business system, through an analog line, Digital Subscriber Line, a LAN, frame relay, asynchronous transfer mode, SONET or wireless connection.
- **Scalability**. A future-proof, flexible, and safe solution combined with high reliability lets your company focus on customer needs, not network problems. Nortel Networks Internet Telephony solutions offer hybrid environments that leverage existing investments in Meridian and Norstar systems.
- **Increased customer satisfaction**. Breakthrough e-business applications help deliver the top-flight customer service that leads to success. By providing your customers rapid access to sales and support personnel via phone, the Web, and e-mail, your business can provide better customer service than ever before.

IP telephones and VoIP trunks

This guide describes two similar applications for IP telephony on the Business Communications Manager system: IP telephones and VoIP trunks. These applications can be used separately or together as a network voice/data solution.

IP telephones

IP telephones offer the functionality of regular telephones, but do not require a hardwire connection to the Business Communications Manager. Instead, they must be plugged into an IP network which is connected to the LAN or WAN card on the Business Communications Manager. Calls made from IP telephones can pass over VoIP trunks or across a Public Switched Telephone Network (PSTN).

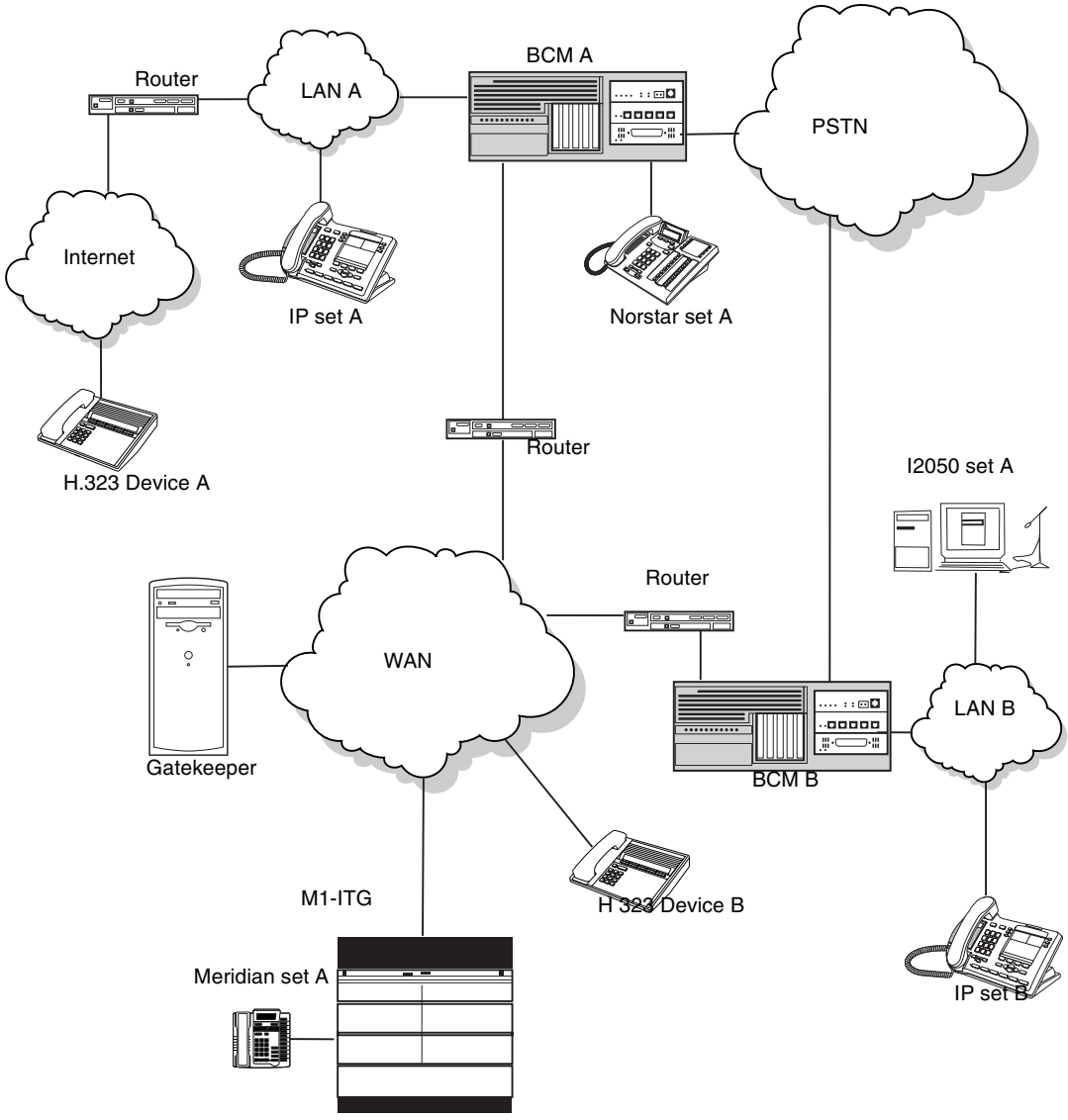
VoIP trunks

VoIP trunks allow voice signals to travel across IP networks. A gateway within the Business Communications Manager converts the voice signal into IP packets, which are then transmitted through the IP network. The device at the other end reassembles the packets into a voice signal.

The IP telephony network

This section explains the components of the Business Communications Manager system and the devices it interoperates with to create a network. Figure 1: Network diagram on page 21 shows components of the Business Communications Manager system.

Figure 1 Network diagram



Business Communications Manager

The Business Communications Manager is a key building block in creating your network. It interoperates with many devices including the M1 and any H.323 device. In this network diagram, the Business Communications Manager system is connected to devices through multiple IP networks as well as the PSTN. Multiple Business Communications Manager systems can be linked together on a network.

In Figure 1: Network diagram on page 21, BCM A is connected to a LAN (via a LAN card), a WAN (via a WAN card), and a PSTN (via Media Bay Modules). Through these networks, the system accesses other systems and network equipment connected to the network.

M1-ITG

The Meridian 1 Internet Telephony Gateway lets the M1 communicate with H.323 devices including the Business Communications Manager. In Figure 1: Network diagram on page 21, telephones on the M1 such as Meridian set A can initiate and receive calls with the other telephones on the system across IP networks.

Telephones

The Business Communications Manager system can communicate using several different types of telephones, ranging from traditional analog and digital telephones to IP telephones and H.323 terminals.

Traditional telephones

While traditional telephones cannot be connected to the Business Communications Manager system with an IP connection, they can useVoIP trunks to make calls to other locations on a network.

IP telephones

Nortel IP telephones include the i2004, i2002 and i2050. These devices connect to the Business Communications Manager across an IP network through either a LAN or a WAN.

H.323 terminals

H.323 terminals include computers that have Microsoft NetMeeting installed, or other third-party devices. These terminals connect through the network to either the LAN or WAN card on the Business Communications Manager.

Gatekeeper

A gatekeeper tracks IP addresses of specified devices, and provides authorization for making and accepting calls for these devices. A gatekeeper is not required for the Business Communications Manager system, but can be useful on networks with a large number of devices. In Figure 1: Network diagram on page 21, for example, when Norstar set A wants to call an H.323 device, and Norstar set B is under the control of the gatekeeper, Norstar set A sends a request to the gatekeeper. The gatekeeper, depending on how it is programmed, provides Norstar set A with the information it needs to contact Norstar set B.

IP Network

In the network shown in Figure 1: Network diagram on page 21 several LANs and a WAN are shown. When planning your network, be sure to consider your other needs for a data network.

WAN

A Wide Area Network (WAN) is a communications network that covers a wide geographic area, such as state or country. For Business Communications Manager, a WAN is any IP network connected to a WAN card on the Business Communications Manager system. This may also be a direct connection to another Business Communications Manager system.

LAN

A Local Area Network (LAN) is a communications network that serves users within a confined geographical area. For Business Communications Manager, a LAN is any IP network connected to a LAN card on the Business Communications Manager system. Often, the LAN can include a router that forms a connection to the Internet.

Public Switched Telephone Network

The Public Switched Telephone Network (PSTN) can play an import role in IP Telephony communications. In many installations, the PSTN forms a fallback route, so that if a call across a VoIP trunk does not have adequate voice quality, the call is routed across the PSTN instead. The Business Communications Manager also serves as a gateway to the PSTN for users on the system.

Key IP Telephony Concepts

In traditional telephony, the voice path between two telephones is circuit switched. This means that the analog or digital connection between the two telephones is dedicated to the call. The voice quality is usually excellent, since there is no other signal to interfere.

In IP telephony, voice quality between IP telephones can vary significantly from call to call and time of day. When two IP telephones are on a call, each IP telephone encodes the speech at the handset microphone into small data packets called frames, and sends the frames across the IP network to the other telephone where the frames are decoded and played at the handset receiver. If some of the frames get lost while in transit, or are delayed too long, the receiving telephone experiences poor voice quality.

Codecs

The algorithm used to compress and decompress voice is embedded in a software entity called a codec (COde-DECode).

Two popular Codecs are G.711 and G.729. The G.711 Codec samples voice at 64 kilobits per second (kbps) while G.729 samples at a far lower rate of 8 kbps.

Voice quality is better when using a G.711 CODEC, but more network bandwidth is used to exchange the voice frames between the telephones.

If you experience poor voice quality and suspect it is due to heavy network traffic, you can get better voice quality by configuring the IP telephone to use a G.729 CODEC.

Jitter Buffer

Voice frames are transmitted at a fixed rate, because the time interval between frames is constant. If the frames arrive at the other end at the same rate, voice quality is perceived as good. In many cases, however, some frames can arrive slightly faster or slower than the other frames. This is called jitter, and degrades the perceived voice quality. To minimize this problem, configure the IP telephone with a jitter buffer for arriving frames. This is how the jitter buffer works:

Assume a jitter buffer setting of five frames.

- The IP telephone firmware places first five arriving frames in the jitter buffer.
- When frame six arrives, the IP telephone firmware places it in the buffer and sends frame one to the handset speaker.
- When frame seven arrives, the IP telephone buffers it and send frame two to the handset speaker.

The net effect of using a jitter buffer is that the arriving packets are delayed slightly in order to ensure a constant rate of arriving frames at the handset speaker. The disadvantage of using a jitter buffer is that the speech arrives delayed by the number of frames in the buffer. For one-sided conversations, this is not an issue. For conversations where one party tries to interrupt the other speaking party, it is annoying because by the time the voice of the interrupter reaches the interruptee, the interruptee has spoken (2*jitter size) frames past the intended point of interruption. In cases where very large jitter sizes are used, some users revert to saying "OVER" when they wish the other party to speak.

Possible jitter buffer settings, and corresponding voice packet latency (delay) for the Business Communications Manager system IP telephones are:

- None
- Small (.06 seconds)
- Medium (.12 seconds)
- Large (.18 seconds)

QoS routing

When it sends a voice frame onto the network, the IP telephone firmware places some header information on the frame.

The header contains the network address of the sending and receiving IP telephones, and a TOS (Type Of Service) byte, which contains a routing priority.

The IP telephone firmware establishes the TOS byte to the highest possible priority so that as the voice frame travels through the network, the routers it encounters give it higher routing priority than competing data frames resulting from file transfers, WEB downloads, e-mails, etc. This process of prioritizing data frames is Quality of Service (QoS) routing.

The Business Communications Manager system does QOS routing, but if one or more routers along the network route do not support QOS routing, this can impact voice quality. Business Communications Manager system QoS can also be configured so that the system reverts to a circuit-switched line if a suitable QoS cannot be guaranteed.

Chapter 2
Prerequisites checklist

Before you set up VoIP trunks or IP telephones on a Business Communications Manager, complete the following checklist to ensure that the system is set up properly. Some questions do not apply to all installations.

Network diagram

To aid in installation a Network Diagram is needed to provide a basic understanding of how the network is configured. Before you install VoIP functionality, you must have a network diagram that captures all of the information described below. If you are configuring IP telephones but not IP trunks, you do not need to answer 1.d and 1.e.

Table 1 Network diagram

Prerequisites	Yes	No
1.a Has a network diagram been developed?		
1.b Does the network diagram contain any routers, switches or bridges with corresponding IP addresses and bandwidth values for WAN or LAN links?		
1.c Does the network diagram contain IP Addresses and network locations of all BCMs?		
1.d Answer this if your system will use IP trunks, otherwise, leave it blank: Does the network diagram contain IP Addresses of any other Voice over IP gateways desired to connect to?		
1.e Answer this only if your system will use a gatekeeper, otherwise, leave it blank: Does the network diagram contain alias for any Gatekeeper that may be used?		

Network devices

This section of the checklist contains questions about devices on the network such as firewalls, NAT devices, and DHCP servers.

Table 2 Network device checklist

Prerequisites	Yes	No
2.a This section of the checklist contains questions about devices on the network such as firewalls, NAT devices, and DHCP servers.		
2.b Is the network using private IP addresses? If the network uses public IP addresses, complete 2.c. If the network uses private IP addresses, complete 2.d to 2.e.		
2.c Are there enough public IP addresses to accommodate all IP telephones and the Business Communications Manager?		
2.d Does the system have a firewall/NAT device, or will the BCM be used as a firewall/ NAT device?		
2.e The Business Communication Manager has limited space fore firewall rules. If the Business Communications Manager is to be used as a firewall/NAT device, do the firewall rules fit within 32 input rules and 32 output rules?		
2.f A hub-based core will not have suitable performance for IP Telephony. Does the network use a non-hub solution at its core?		

Network assessment

This section ensures that the network is capable of handling IP Telephony and that existing network services are not adversely affected.

Table 3 Network assessment

Prerequisites	Yes	No
3.a Has a network assessment been completed?		
3.b Has the number of switch/hub ports available and used in the LAN infrastructure been calculated?		
3.c Have the used and available IP addresses for each LAN segment been calculated?		
3.d Has DHCP usage and location been recorded?		
3.e Has the speed and configuration of the LAN been calculated?		
3.f Has the estimated latency values between network locations been calculated?		
3.g Bandwidth/CIR utilization values for all WAN links.		
3.h Has the quality of service availability on the network been calculated?		

Resource Assessment

You must allocate sufficient resources on the Business Communications Manager for IP telephony.

Table 4 Resource Assessment

Prerequisites	Yes	No
4.a Has a Business Communications Manager Resource Assessment been performed using the resource questionnaire in the Programming Operations Guide?		
4.b Has an analysis been done to determine which DS-30 split is appropriate for the system, and has the DS-30 split been changed to 5/3 if necessary?		
4.c Have all necessary media resources for IP trunks, clients, vmail or WAN dialup been assigned or dedicated?		

Keycodes

All elements of VoIP trunks and IP telephony are locked by the Business Communications Manager keycode system.

Table 5 Keycodes

Prerequisites	Yes	No
5.a Complete this question only if you are using VoIP trunks: Do you have enough VoIP keycodes?		
5.b Complete this question only if you are using IP telephones: Do you have enough IP client keycode?		

Business Communications Manager System Configuration

Several sections of the the Business Communications Manager must be properly configured prior to activation of IP telephony.

Table 6 Business Communications Manager system configuration

Prerequisites	Yes	No
6.a Is the LAN functioning properly with the Business Communications Manager?		
6.b Is the WAN functioning properly with the Business Communications Manager?		
6.c Has a dialing plan been created, taking into account special considerations for IP telephony?		
6.d Has a preference been established between pre-configured DNs and auto-assigned DNs? If the preference is for auto-assigned DNs, complete 6.e.		
6.e Complete this question only if you are not using Auto-assign DNs. Have set DNs been programmed for the corresponding IP clients?		

IP Telephones

Complete this section only if you have IP telephones.

Table 7 IP telephones

Prerequisites	Yes	No
7.a Are IP connections and IP addresses available for all IP telephones?		
7.b If DHCP is not being used, has all telephone configuration been documented and made available for telephone installers?		
7.c Has telephone powering been provisioned?		
7.d Do computers that will be using the i2050 soft phone meet the minimum system requirements, including headset?		
7.e Are IP connections and IP addresses available for all IP telephones?		

Chapter 3
Installing IP Telephones

An IP telephone converts the voice signal into data packets and sends these packets directly to another IP telephone or to the Business Communications Manager. If the destination is an IP telephone, the arriving voice packets are converted to a voice stream which is routed to a speaker or headset. If the destination is the Business Communications Manager, the voice stream is routed to a circuit switched connection (telephone or line), or some form of gateway.

Note: IP telephones require an IP network to reach the Business Communications Manager. However, they do not need to use VoIP trunks to communicate beyond the Business Communications Manager. They can use any type of trunk, just as any other phone on the Business Communications Manager can.

Before setting up IP clients, you must enable keycodes for IP telephony. For information on entering keycodes, see the *Keycode Installation Guide.*

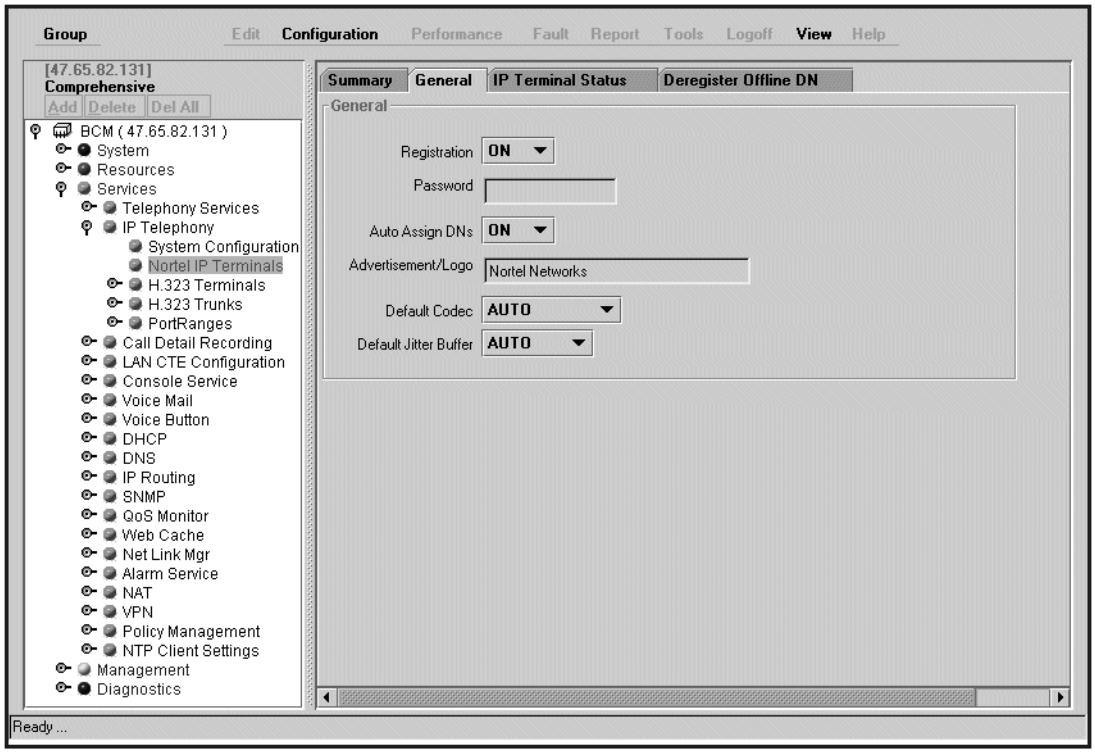
Preparing your Business Communications Manager for IP telephone registration

If this is the first time you are installing an IP telephone on this Business Communications Manager, you must activate terminal registration on the Business Communications Manager.

Note: For the simplest installation possible, set telephone Registration and Auto Assign DNs to ON, and leave Password blank. IP Telephones installed on the system will connect and boot-up without manual registration.

1 In Unified Manager, open **Services**, **IP Telephony**, and **Nortel IP Terminals**. Select the **General** tab:

Figure 2 Set registration properties



2 Set **Registration** to **ON** to allow new IP clients to register with the Business Communications Manager.

Note: For security reasons, set the Registration to Off when you are not registering telephones.

3 In the **Password** box, type a password. This is the password that installers must enter from the IP terminals to connect to the Business Communications Manager. If this field is left blank, no password is needed to register an IP terminal.

Note: The default password is “bcmi”. It can be changed to any alphanumeric string that is 10 characters in length or less.

4 Set the **Auto Assign DN** box. If Auto Assign DNs is set to ON, the Business Communications Manager system assigns a free DN to a set being registered instead of prompting the installer for the set DN. If registration and Auto Assign DNs are both set to ON, and the Registration password is blank, first-time-connected IP clients will be assigned a DN without requiring installer intervention. The system selects this number from the Norstar Digital Telephone Range.

5 In the **Advertisement/Logo** box, type a string of text characters. This message is displayed on the first line of the IP terminal’s display. This string can be a maximum of 24 characters.

6 From the **Codec** menu, select a default Codec, or leave the Default Codec at Auto. This is the Codec that is used if an IP telephone has not been configured with a preferred codec. For information on this, see "Choosing a codec" on page 33.

7 From the **Jitter Buffer** menu, select a Jitter Buffer level. For information on choosing a Jitter Buffer, see "Choosing a Jitter Buffer" on page 33.

Choosing a codec

The default codec is used when an IP client has not been configured to use a preferred Codec (see the next section for individual IP client Codec settings). If the default Codec is set to AUTO, the Business Communications Manager will choose the appropriate CODEC when an IP client goes on a call. For example, if both endpoints of the call are I20XX telephones on the same subnet, the Business Communications Manager chooses G.711 for maximum voice quality. If the telephones are on different subnets, the Business Communications Manager will choose G.729 to minimize network bandwidth consumption by voice data packets.

For IP telephones, the Business Communications Manager supports both A and MU law variants of the G.711 CODEC, as well as the G.729 and G.723 CODECS.

- The G.711 CODEC samples the voice stream at a rate of 64Kbps (Kilo bits per second), and is the CODEC to use for maximum voice quality.
- The G.729 CODEC samples the voice stream at 8Kbps. The voice quality is slightly lower using a G.729 but it reduces network traffic by approximately 80%.
- The G.723 CODEC should be used only with third party devices that do not support G.729 or G.711.

Choosing a Jitter Buffer

A jitter buffer is used to prevent the jitter associated with arriving (Rx) voice packets at the IP telephones. The jitter is caused by packets arriving out of order due to having used different network paths, and varying arrival rates of consecutive voice packets.The greater the size of the jitter buffer, the "better sounding" the received voice is. However, voice latency (delay) also increases. Latency is very problematic for telephone calls, as it increases the time between when one user speaks and the user at the other end hears the voice. The administrator can adjust the default jitter buffer size to the following values:

- NONE: Minimal latency, best for short-haul networks with good bandwidth.
- AUTO: Business Communications Manager will dynamically adjust the size.
- SMALL: Business Communications Manager will adjust the buffer size, depending on CODEC type and number of frames per packet to introduce a 60 millisecond delay.
- MEDIUM: 120 millisecond delay
- LARGE: 180 millisecond delay

Installing and Configuring i2004 Internet Telephones

The telephone can be configured by the end user or by the administrator. If the end user is configuring the telephone, the administrator must provide the user with parameters to configure.

A maximum of 90 IP telephones, softphones and H.323 units can be connected on the Business Communications Manager system.

Before Installing

Before installing the i2004 telephone, ensure that:

- the installation site has a 120V AC (60 Hz) outlet
- the installation site has a 10/100 BaseT Ethernet connection
- If you are not using the 3-port switch, you must have an additional 10/100 BaseT Ethernet connection connecting you to the local Ethernet.

Using a 3-port switch

In an office environment where a LAN network already exists, most computers will already be connected to a LAN line. Using the Nortel Networks 3-port switch, the i2004 phone can be installed on the network along with the computer, without needing to add an extra cable to a hub. For more information, consult the i2004 documentation.

Connecting the i2004 Internet telephone

Caution: Do not plug the telephone into an ISDN connection. This can cause severe damage to the telephone. Plug the telephone into only a 10/100 BaseT Ethernet connection

To connect the i2004 Internet telephone:

1. Connect one end of the handset cord to the handset jack on the telephone base. Connect the other end of the handset cord to the handset.
2. Connect one end of a Cat-5 line cordwith RJ45 connectors to the line cord jack on the telephone base. Connect the other end of the line cord to the Ethernet connection.
3. Plug the AC Power adapter into the base of the telephone, and plug the adapter into the AC outlet.

Configuring the i2004 telephone

Depending on how you set up terminal registration, you may be prompted for the password and a DN for the telephone the first time the telephone is booted. For information on setting the registration settings, see "Preparing your Business Communications Manager for IP telephone registration" on page 31.

1. If the telephone is not yet registered, and if a password was entered in the Terminal Registration screen, the telephone prompts you for that password. Type the password.
2. If you set Auto Assign DN on the Business Communications Manager to OFF, the telephone prompts you for a DN. Choose a DN for the telephone. Entering '0' will cause the system to automatically assign a DN to the telephone.

Once registration has been completed, you do not need to go through the registration steps described above unless you deregister a terminal.

To access the local configuration menu on a i2004 telephone:

1. Restart the telephone by disconnecting then reconnecting the power. After about four seconds, the top light flashes and 'NORTEL NETWORKS' appears on the screen.
2. When the greeting appears, press the four softkeys (located under the telephone's display) one at a time from left to right. These keys must be pressed one after the other within 1.5 seconds, or the telephone will not go into configuration mode.
   If '`Manual Cfg DHCP(0 no, 1 yes)`' appears on the screen, you successfully accessed the configuration mode.
   If '`Manual Cfg DHCP(0 no, 1 yes)`' does not appear, disconnect then reconnect the power, and try to access the configuration mode again.
3. For each parameter, use the keypad to define values. Refer to Table 8 on page 35 for information on each parameter.To type a decimal, press *.

Table 8 Settings for IP telephones

DHCP	0 if not using a DHCP server to disperse IP addresses 1 if using a DHCP server If you choose to use a DHCP server rather than allocating static IP addresses for the IP telephones, skip the remainder of this section. For information on setting up a DHCP server, see "Configuring DHCP" on page 38.
SET IP	The set IP must be a valid and unused IP address.
NETMASK	This is the subnet mask

DEF GW	Default Gateway on the network (i.e., the nearest router to the telephone. The router for IP address W.X.Y.Z is usually at W.X.Y.1) If there are no routers between the telephone and the Business Communications Manager network adaptor to which it is connected, (for example a direct HUB connection), then enter the Published IP address of the Business Communications Manager as the DEF GW. If the IP telephone is not connected directly to the Published IP address network adaptor, set the DEF GW to the IP address of the network adaptor the telephone is connected to. For information on setting the published IP address of the Business Communications Manager, see "Setting the Published IP Address" on page 51.
S1 IP	This is the Published IP address of the Business Communications Manager.
S1 PORT	Set this to 7000.
S1 ACTION	Set this to 1.
S1 RETRY COUNT	Set this to 255.
S2 IP	This is the Published IP address of the Business Communications Manager.
S2 PORT	Set this to 7000.
S2 ACTION	Set this to 1.
S2 RETRY COUNT	Set this to 255.

After you have configured a telephone, it attempts to connect to the Business Communications Manager. The message 'Locating Server' appears on the display. If the connection is successful, the message changes to 'Connecting to Server' after about 15 seconds.

The IP telephone is completely booted once the date/time string is displayed on the telephone. Do not attempt to use the telephone while the string "Connecting to server" is displayed (initialization of the telephone may take several minutes).

Troubleshooting an IP telephone

If the system is not properly configured, several messages can appear:

- SERVER: NO PORTS LEFT--The Business Communications Manager has run out of ports. This message will remain on the display until a port becomes available and the telephone is powered down then powered up.To obtain more ports, you may need to install additional keycodes. See the *Keycode Installation Guide.*
- Invalid Server Address--The S1 is incorrectly configured with the IP address of a Business Communications Manager network adapter other than the published IP address.
- NEW SET--The telephone has not been connected to the Business Communications Manager before, and must be registered.

- Registration Disabled--The Registration on the Business Communications Manager is set to OFF.

Note: To see the configuration information of a telephone connected to the Business Communications Manager:

When the telephone is not on a call, press the EXPAND key (blue key at the bottom-right of the telephone) followed by the SERVICES key (key with image of a globe).

To see the Codec data for a telephone while it is on a call:
Press the EXPAND key (blue key at the bottom-right of the telephone) followed by the SERVICES key (key with image of a globe).

Use the following strategies for troubleshooting an IP telephone:

- If an IP telephone does not boot, use VNC to access the Business Communications Manager. Find this file: `E:\NORTEL NETWORKS\Logs\Nnu\UTPS.log`.
  If the telephone is properly configured to reach the Business Communications Manager, you should see this message in the log: "Opening signaling channel for set index X [at A.B.C.D]" where A.B.C.D is the telephone's IP address.

If this entry is not present, the IP telephone is not connected to the Business Communications Manager. Double check the telephone configuration parameters. VNC into the Business Communications Manager, open a DOS window and try pinging the telephone. Check the configuration settings of any NAT server, DHCP server, firewall and routers between the telephone and the Business Communications Manager. For information on using Ping, see Appendix C, "Network Performance Utilities," on page 109.

- While signaling between the IP telephones and the Business Communications Manager uses Business Communications Manager port 7000, voice packets are exchanged using the default RTP ports 28000 through 28255 at the Business Communications Manager, and ports 51000 through 51200 at the IP telephones. If these ports are blocked by the firewall or NAT, you will experience one-way or no-way speech paths.
- If the LAN traffic in your network environment is heavy, you may experience dropped voice packets. If this occurs, connect the Business Communications Manager and the telephones to a local network hub to avoid the network traffic.
- If an IP telephone does not display the text "Connecting to server" within two minutes after power up, the telephone was unable to establish communications with the Business Communications Manager. Double check the telephone's IP configuration, and IP connectivity to the Business Communications Manager (cables, hubs, etc.).
- When an IP telephone is connected for the first time, the contrast level is set to the default setting of 1. Most users find this value is too low. Therefore, after the telephone is operational, you can increase the contrast level by pressing Feature *7 at the telephone.
- If the connection between the IP client and the Business Communications Manager is slow (ISDN, dialup modem), change the preferred CODEC for the telephone from G.711 to G.729. (See "Settings for IP telephones" on page 35.)

Configuring DHCP

An alternative to manually configuring the IP sets is to use Distributed Host Control Protocol (DHCP) to automatically assign IP addresses to the IP sets. Before setting up DHCP using the information below, see the *Business Communications Manager 2.5 Programming Operations Guide* for more extensive information on DHCP.

Note: Do not enable DHCP on the BCM if you have another DHCP server on the network

To set up DHCP to work with IP terminals, ensure that DHCP is set up with the following settings:

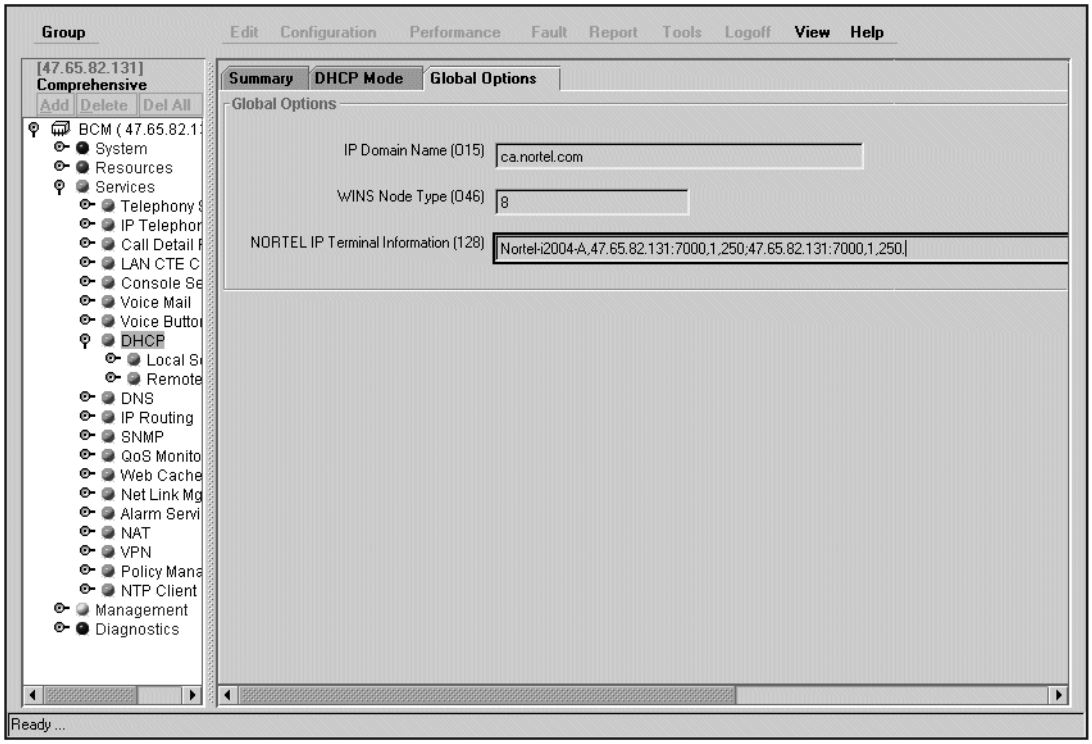
1 In Unified Manager, navigate to **Services/DHCP**, and select the **Global Options** tab. The Global Options screen appears.

2 Set the NORTEL IP Terminal Information box to:

```
Nortel-i2004-A, iii.jjj.kkk.lll:7000,1,250;iii.jjj.kkk.lll:7000,1,250.
```

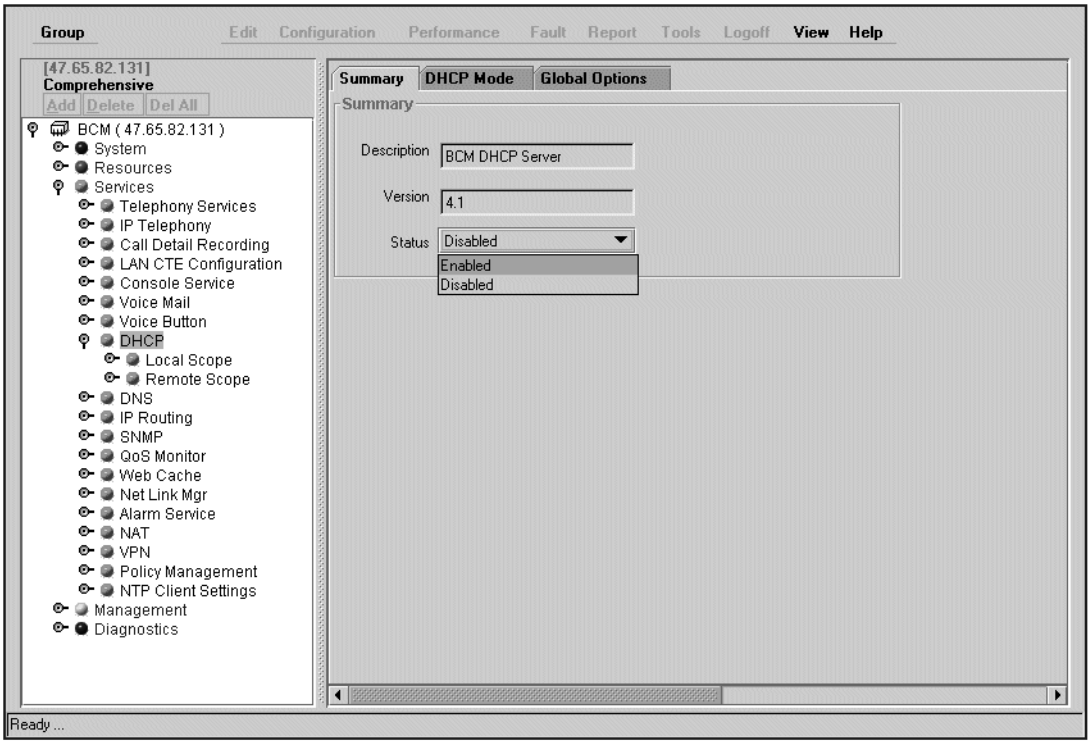
iii.jjj.kkk.lll represents the published IP address. Be sure to include the period at the end of the string (1,250.). In Figure 3, 47.65.82.131 is the published IP address:

Figure 3 Global options



3 Click the **Summary** tab. The summary screen appears:

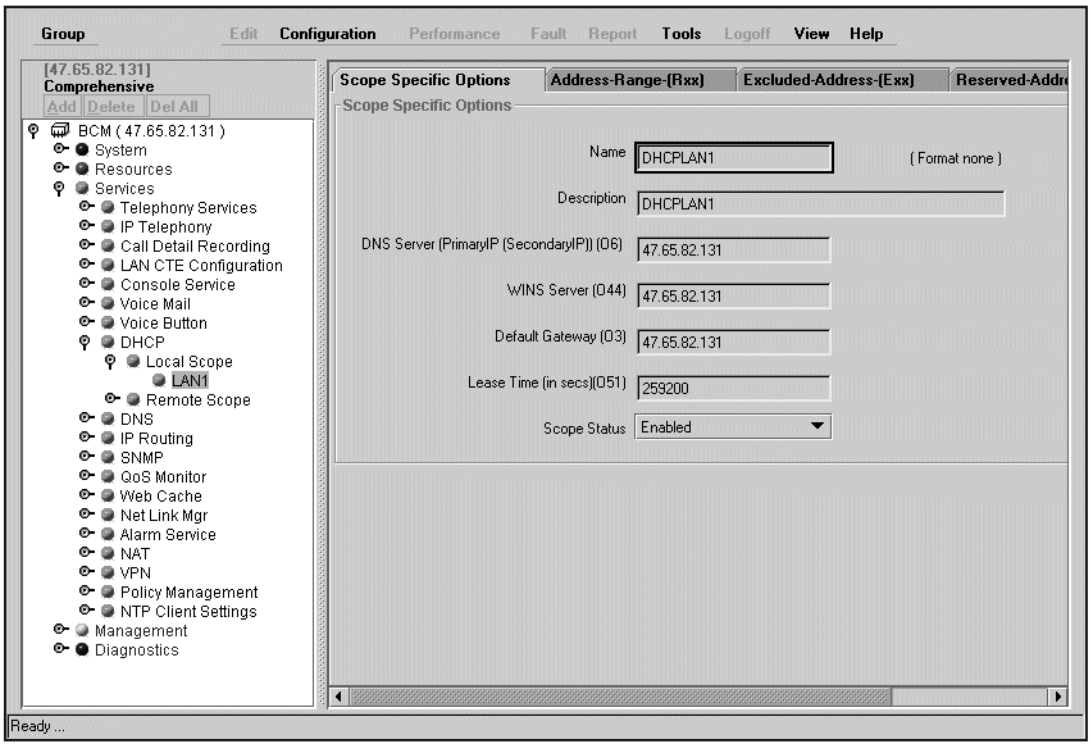
Figure 4 DHCP summary



4 Set the **Status** box to **Enabled**.

5 Open **Services/DHCP/Local Scope/LANX**, where LANX is a LAN that contains IP sets that use DHCP. The Scope Specific Options Screen appears:

Figure 5 DHCP range



6 Set each of the following:

- **Scope Status**: set this to **Enabled**
- **Default Gateway Field**: set this to Published IP Address.
- **Address Range**: set the range of IP addresses the DHCP server dispenses.

7 Repeat Step 6 for every network adapter that IP sets use to connect to the Business Communications Manager.

8 Restart all of the IP telephones.

Note: Whenever changes are made to the DHCP settings, telephones will retain the old settings until they are restarted.

If the DHCP server is not properly configured with the Published IP address, the telephones will display “Invalid Server Address”. You must then correct the DHCP settings, and restart the telephones.

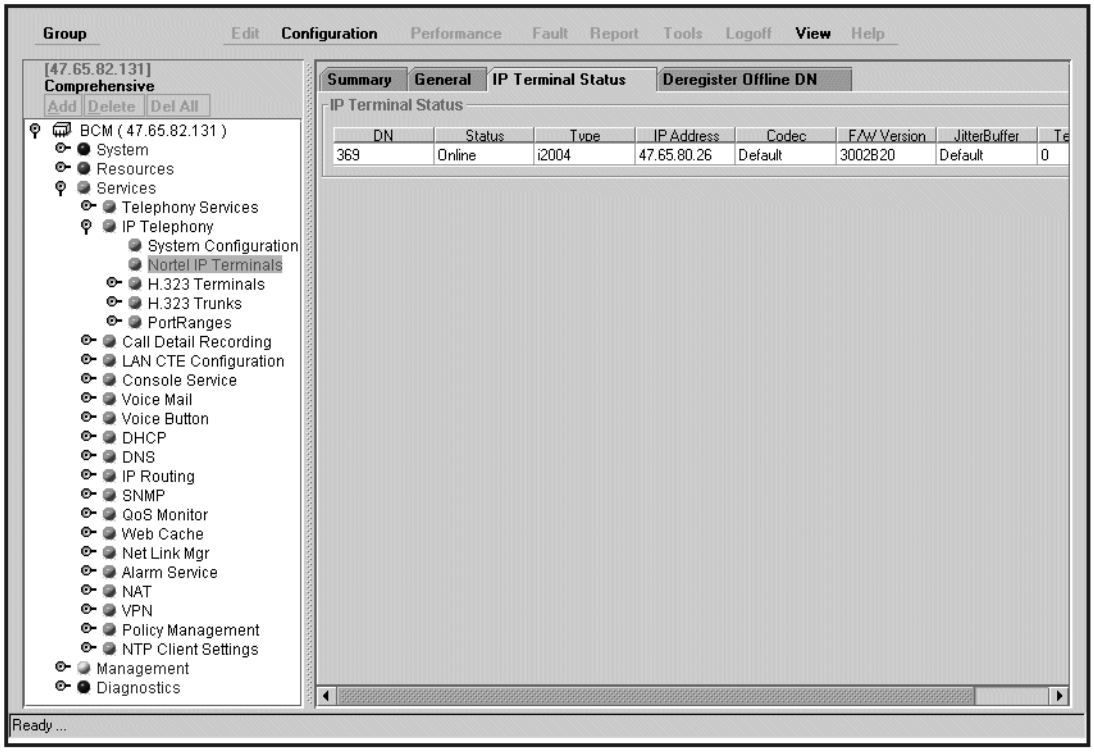
Modifying settings for Nortel IP telephones

Settings such as jitter buffers and codecs for the Nortel IP telephones including the i2050, i2002 and i2004 can be modified through the Unified Manager:

1 In the Unified Manager, open **Services**, **IP Telephony**, and click on **Nortel IP Terminals**. The IP Terminal summary appears.

2 Click on the **IP Terminal Status** tab. Every IP telephone currently connected to the Business Communications Manager occupies a row in the IP Terminal Status table.

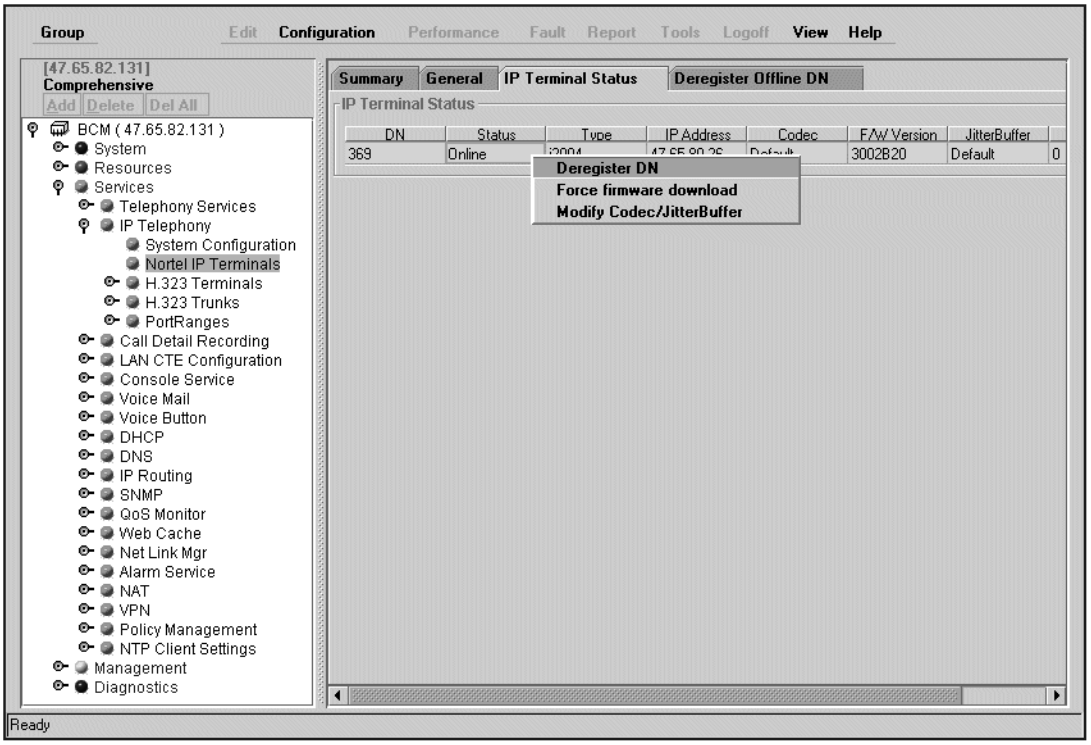
Figure 6 IP Terminal status



3 Select the IP Terminal that you want to change the properties for.

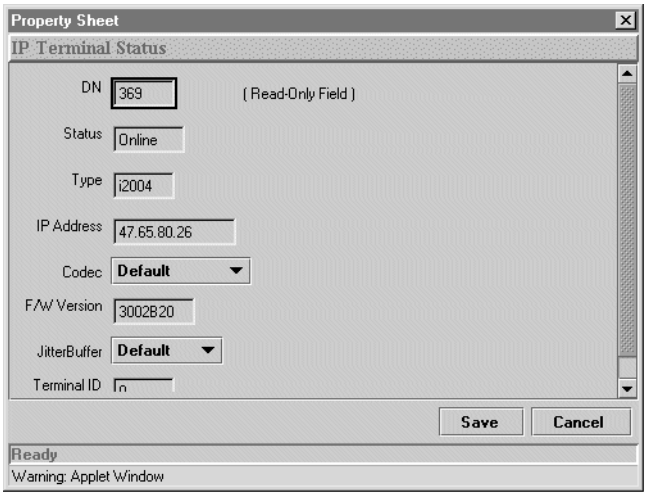
4 Open the **Configuration** menu, or right-click anywhere on the listing for the terminal to bring up the menu.

Figure 7 Configuration menu



5 From the menu, select **Modify Codec/Jitter Buffer**. The Terminal dialog box appears:

Figure 8 Terminal status dialog



6 From the **Codec** menu, select a Codec. Specifying a non-default CODEC for a telephone allows you to override the general setting. You might for example want to specify a low bandwidth CODEC (g.729) for a telephone that is on a remote or busy sub-net.

7 From the **Jitter Buffer** menu, select a jitter buffer value. For a telephone that has poor network connectivity to the Business Communications Manager, increase the jitter buffer size.

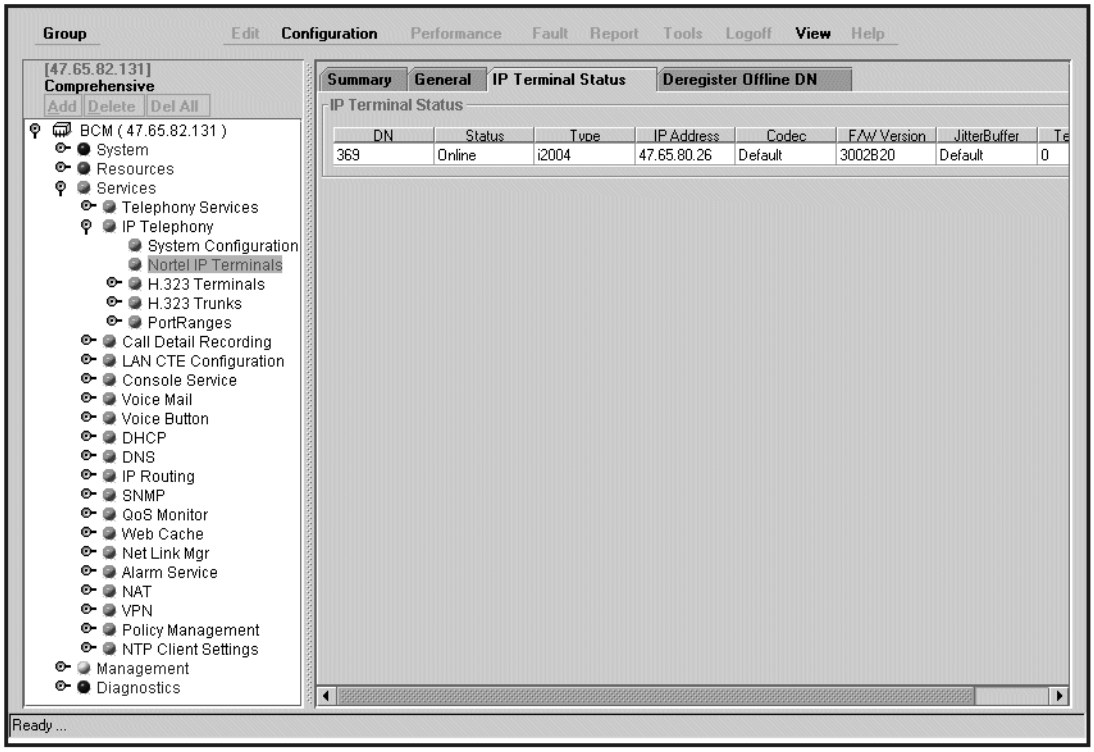
Download Firmware to an i200X telephone

Firmware is the software stored in the telephone. When the Business Communications Manager is upgraded with a new IP telephone firmware load, this firmware load will automatically be downloaded into the IP telephones when they next connect to the Business Communications Manager. You can use the "Force firmware download" option to force immediate download to a telephone, or if you suspect that a particular telephone has corrupted firmware.

To download firmware to a telephone:

1. In the Unified Manager, open **Services**, **IP Telephony**, and click on **Nortel IP Terminals**. The IP Terminal summary appears.
2. Click on the **IP Terminal Status** tab.

Figure 9 IP Terminal Status



3. Select the IP telephone that you want to download firmware to.
4. Open the **Configuration** menu, or right-click anywhere on the listing for the terminal to bring up the menu.
5. Select **Force Firmware Download**. A dialog appears asking if you want to confirm that you want to proceed.
6. Click the **Yes** button. The firmware download begins.

The system drops any active call on that telephone, and downloads a new firmware load into the selected telephones. The telephones will be unusable until the download is completed and the telephones have reset.

Note: In order not to saturate the IP network with download packets, the system will only download up to five IP telephones at any given time. Telephones requiring download will show a Unified Manager status of `Download Pending`, and the Unistem Trunk Proxy Server (UTPS) will initiate download as resources become available.

Deregistering DNs for online IP telephones

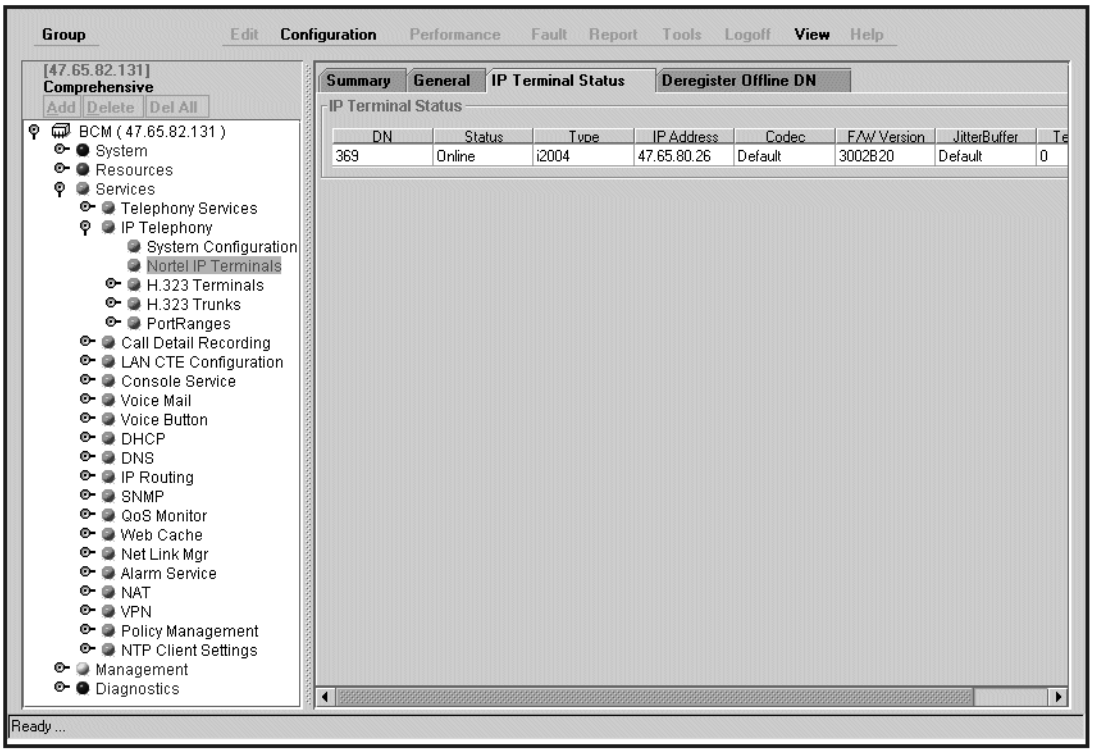
This command will deregister the selected telephones(s) from the Business Communications Manager, and force it to go through the registration process again. Any active calls are dropped.

To deregister a DN for a phone that is online:

1 In the Unified Manager, open **Services**, **IP Telephony**, and click on **Nortel IP Terminals**. The IP Terminal summary appears.

2 Click on the **IP Terminal Status** tab:

Figure 10 IP Terminal Status



3 Select the IP Terminal with the DN you want to deregister.

4 Open the **Configuration** menu, or right-click anywhere on the listing for the terminal to bring up the menu.

5 Click **Deregister DN**.

The **Deregister DN** option deregisters the selected telephone from the Business Communications Manager, and forces it to go through the registration process again. It will cause any active call to be dropped.

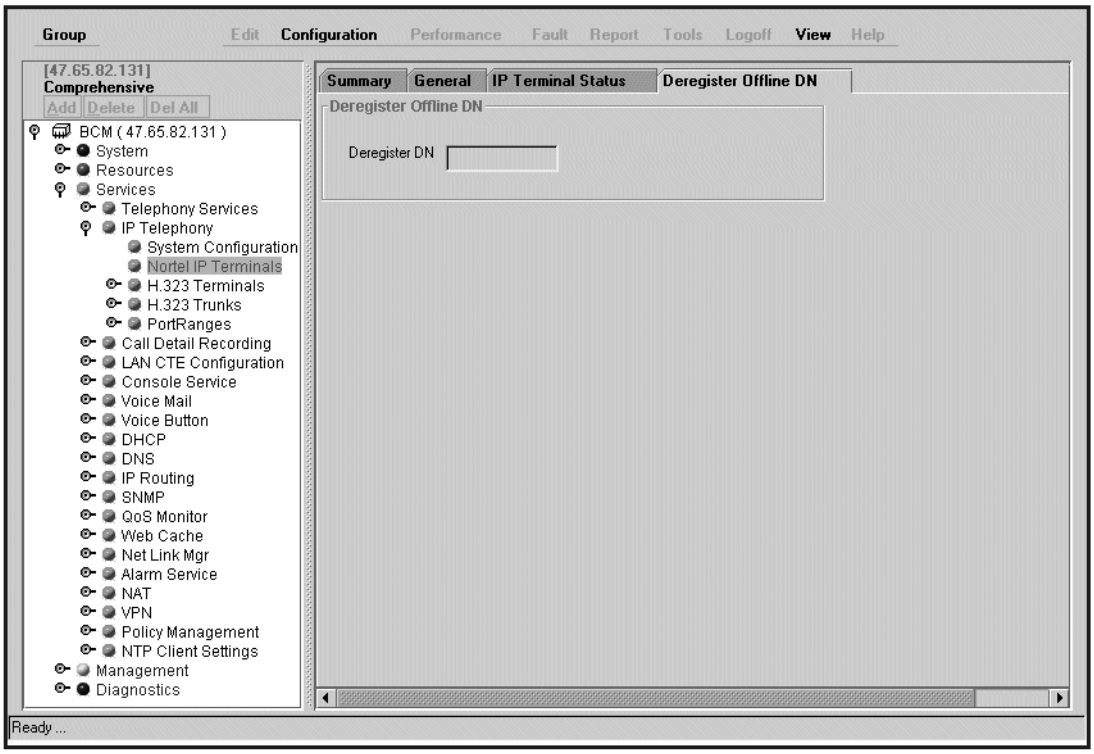
Deregistering offline DNs

To deregister the DN of an IP client that is offline:

1 In Unified Manager, open **Services**, **IP Telephony**, and click on **Nortel IP Terminals**. The IP Terminal summary appears.

2 Click the **Deregister Offline DN** tab. The Deregister Offline DN screen appears:

Figure 11 Deregister Offline DN



3 In the **Deregister DN** field, type the number of the DN you want to deregister.

4 Press **Enter**.
The DN is deregistered.

Moving IP telephones

IP telephones retain their DN when they are moved to a new location. The following instructions apply to I200X phones, computers with the I2050 softphone installed, and H.323 devices.

To move an IP telephone without changing the DN:

1. Disconnect the power from the IP telephone or 3-port switch.
2. Disconnect the network connection.
3. At the new location, reconnect the network location and the power connection.
4. If the new location is on a different LAN or WAN from the old location, the subnet mask, default gateway IP, S1 IP, and S2 IP may change. If this is the case, you must change the settings for the telephone. To do this, see "Connecting the i2004 Internet telephone" on page 34. Do not change the Set IP Address.

To move an IP telephone and change the DN:

1. Deregister the DN, using the instructions in "Deregistering DNs for online IP telephones" on page 44.
2. Disconnect the network connection and the power connection from the telephone.
3. Reinstall the phone at the new location. For information on this, see "Connecting the i2004 Internet telephone" on page 34.

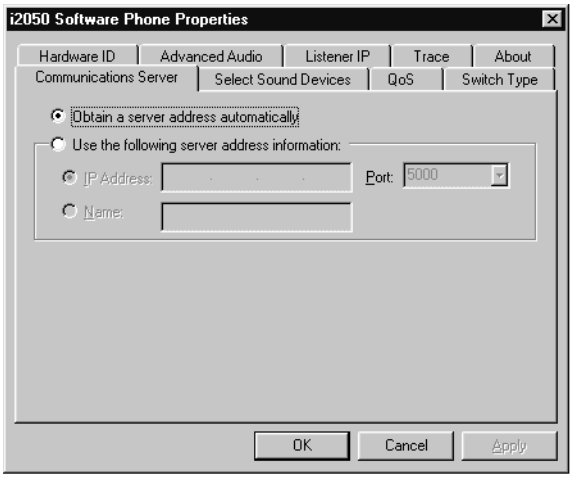
Configuring the i2050 Software Phone

The i2050 Software Phone allows a computer equipped with a soundcard, microphone, and headset to function as an IP terminal on the Business Communications Manager system. The i2050 Software Phone uses the computer's IP network connection to connect to the Business Communications Manager. When you install the i2050 Software Phone, on-screen documentation walks you through the steps for installing the software.

To configure the i2050 Software Phone to connect to the Business Communications Manager:

1. Follow the installation steps for installing your i2050 Software Phone until the software configuration utility appears, or select the software configuration utility from your Windows Start Menu. The utility opens to the Communications Server tab.

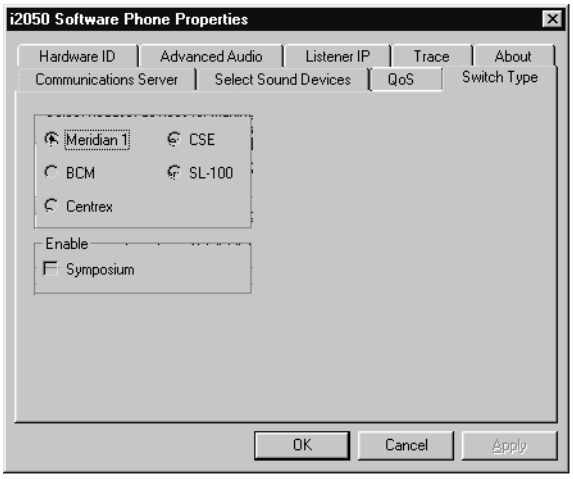
Figure 12 i2050 Communications server



2 Enter the Published IP address of the Business Communications Manager in the **IP address** field.Iin the Port drop down menu, select **BCM** .

3 Select the **Switch Type** tab:

Figure 13 i2050 Switch type



4 Click on the **BCM** option.

5 If using a USB headset, enable it in the **Select Sound Devices** tab.

To further configure this device through Unified Manager, see "Modifying settings for Nortel IP telephones" on page 40.

H.323 devices

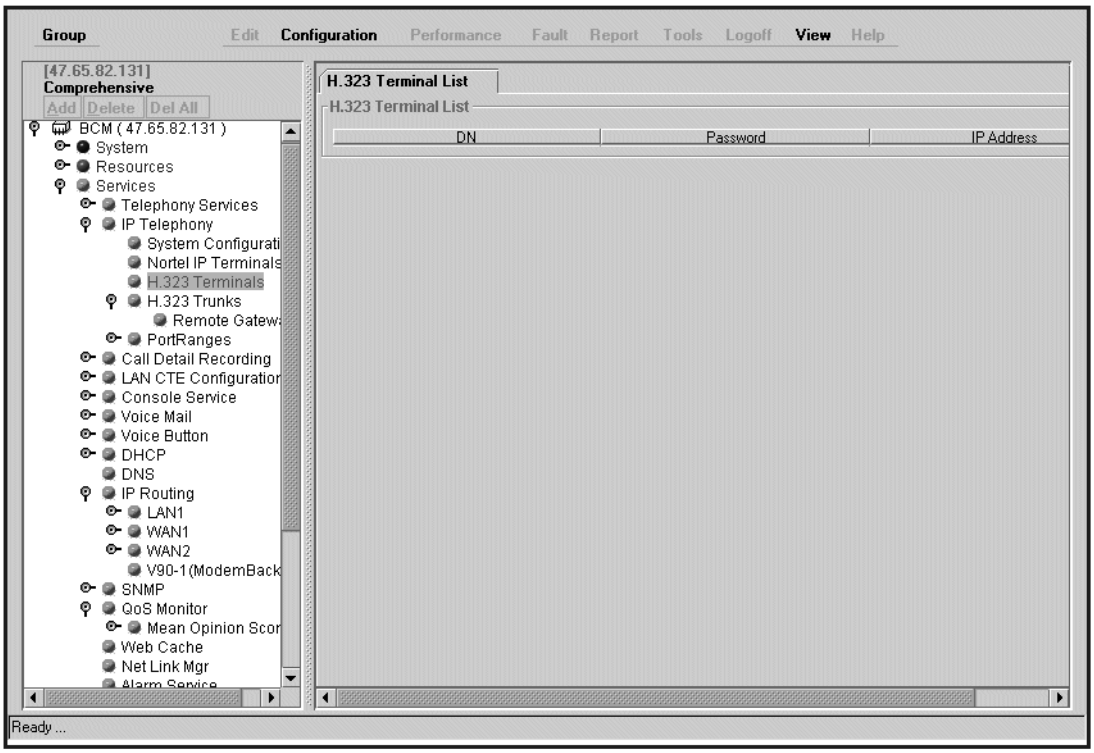
An H.323 device is any device that uses the H.323 protocol. This is a protocol for Internet communications that uses audio, video or data signals.

Adding H.323 devices to the system

The Business Communications Manager can support devices that use the H.323 protocol.To install one of these devices:

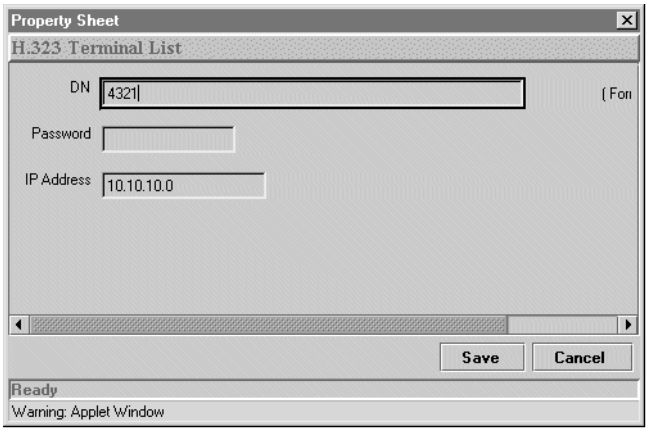
1 In the Unified Manager, open **Services, IP Telephony**, and click on **H.323 Terminals**. The H.323 terminal list appears.

Figure 14 H.323 Terminal list



2 In the **Configuration** menu, click **Add DN**. The H.323 Terminal List dialog appears.

Figure 15 H.323 Terminal list dialog



3 Type a valid DN, password, and the IP address of the terminal.

4 Click the **Save** button.

5 Connect the H.323 device to the network, and use the documentation available with that device to install it.

Chapter 4
VoIP Trunk Configuration

This chapter explains how to configure VoIP trunks on a Business Communications Manager. A VoIP trunk allows you to establish communications between a Business Communications Manager and a remote system across an IP network.

Note: VoIP trunks can be used for calls originating from any type of phone on the Business Communications Manager system. They are not strictly for use with IP terminals.

Configuring a VoIP trunk requires the following actions:

- Installing keycodes
- Configuring media parameters
- Outgoing call configuration
- Incoming call configuration

Note: If you are using the Business Communications Manager with an M1, you must set up the system to be compatible with the M1. See Appendix D, “Interoperability,” on page 111.

Installing keycodes

Before you can use VoIP, you must obtain and install the necessary keycodes. See the Keycode Installation Guide for more information.

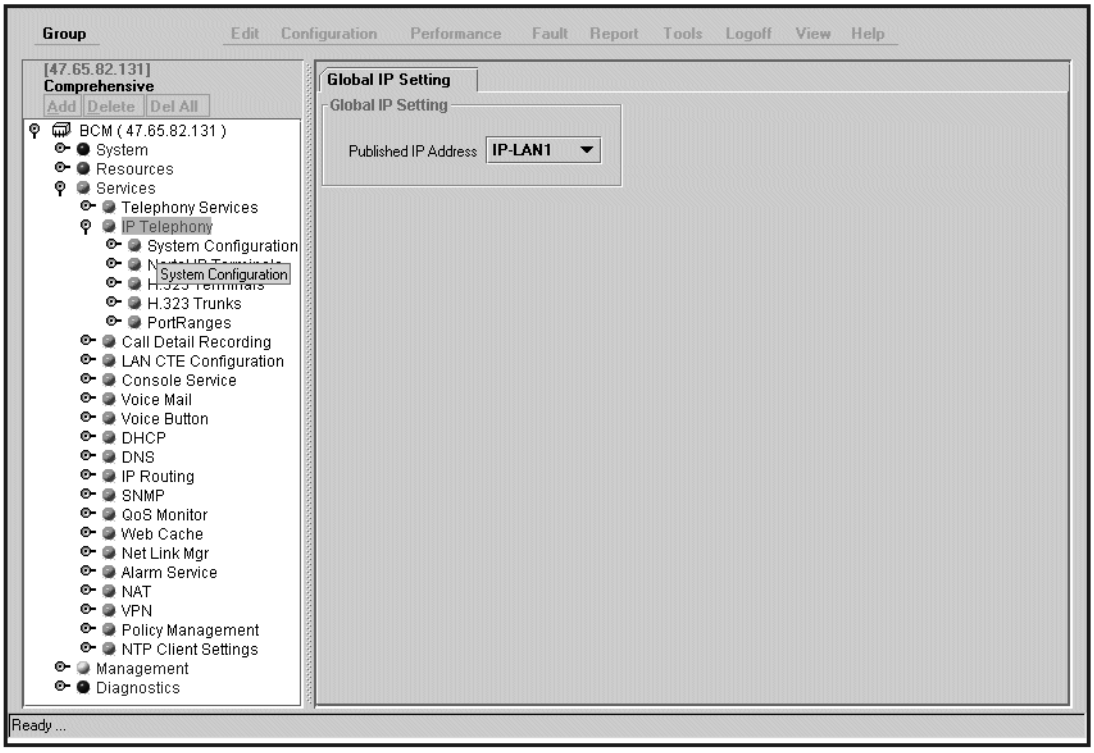
Setting the Published IP Address

The published IP address is the IP address used by computers on the public network to find the Business Communications Manager. For example, if a Business Communications Manager has a LAN interface (LAN1) that is connected only to local office IP terminals and a WAN interface (WAN1) that is connected to the public network, then WAN1 should be set to the published IP address.

To set the published IP address:

1 In Unified Manager, open **Services** and click on **IP Telephony**. The Global settings tab appears.

Figure 16 Global IP settings

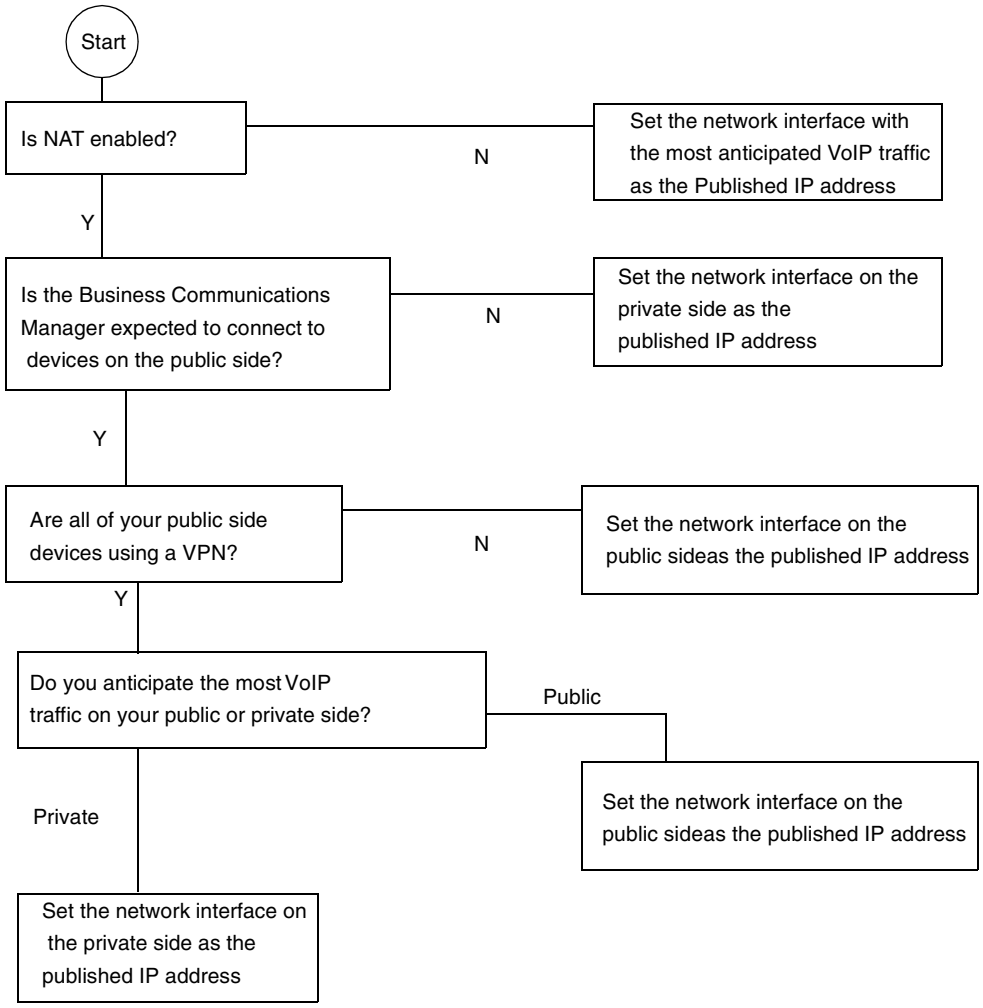


2 From the **Published Address** menu, select the appropriate network interface.

Determining the published IP address

Use the flowchart below to determine which card should be set as the published IP address. The flowchart makes reference to public and private IP addresses. The public and private IP addresses are concepts relating to Network Address Translation (NAT). The decision also depends on whether a Virtual Private Network (VPN) is enabled. For information on NAT, see the *Business Communications Manager 2.5 Programming Operations Guide.*

Figure 17 Setting the Published IP address


Start
Is NAT enabled?
N
Set the network interface with the most anticipated VoIP traffic as the Published IP address
Y
Is the Business Communications Manager expected to connect to devices on the public side?
N
Set the network interface on the private side as the published IP address
Y
Are all of your public side devices using a VPN?
N
Set the network interface on the public sideas the published IP address
Y
Do you anticipate the most VoIP traffic on your public or private side?
Public
Set the network interface on the public sideas the published IP address
Private
Set the network interface on the private side as the published IP address

If you using IP telephones on the network, they must be set to have the IP address of the network card they are connected to for their Default Gateway, and the Published IP address as the S1 IP address. For more information about this, see "Configuring the i2004 telephone" on page 35.

Configuring media parameters

There are three steps to configuring media parameters:

- Configuring codecs
- Setting Silence Compression
- Setting Jitter Buffers

Configuring codecs

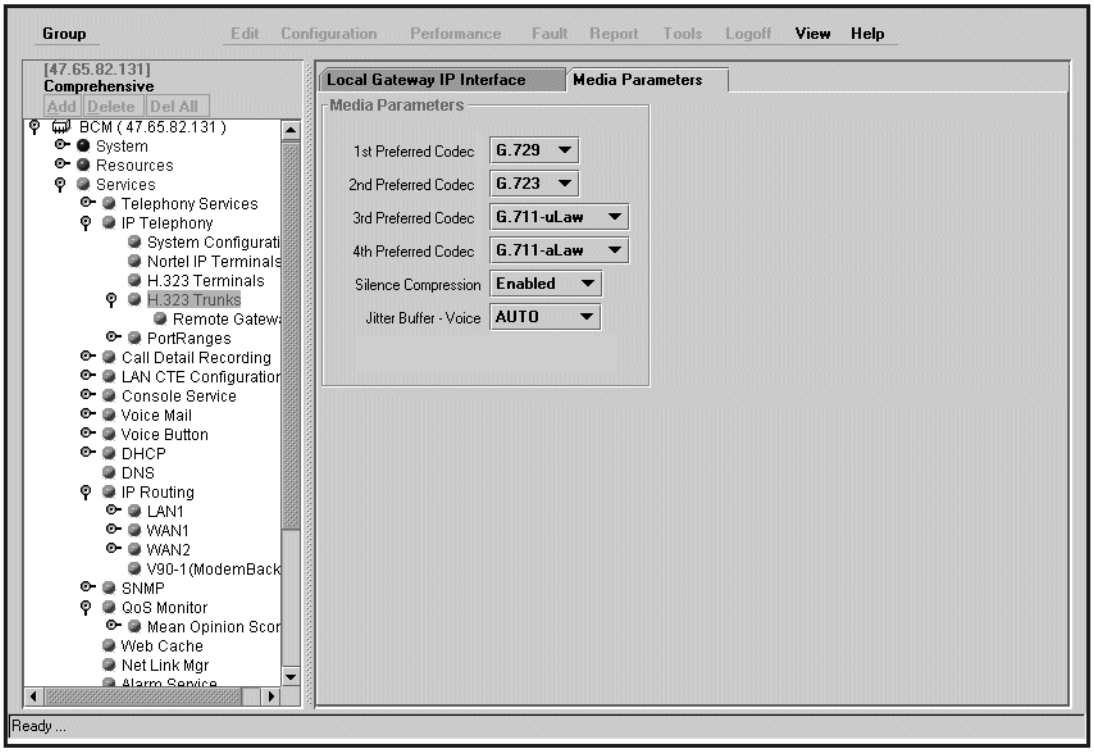
This section explains how to select the codecs that are used for VoIP trunks. For an explanation of codecs, see "Codecs" on page 23.

To configure the codecs:

1 In Unified Manager, open **Services**, **IP Telephony**, and click on **H.323 trunks**.

2 Click on the **Media Parameters** tab. The Media Parameters dialog appears.

Figure 18 Media parameters



3 Click the **First Preferred Codec** menu. Select the codec you want to use as the first preferred codec. This is the most preferred codec to be used on VoIP trunks.

4 For each preferred codec, use the process described in step 3.

Setting Silence Compression

This section explains how to set silence compression on VoIP trunks.

The silence compression feature identifies periods of silence in a conversation, and stops sending IP speech packets during those periods. In a typical phone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. If silence compression is enabled, no voice packets are sent from the listener's end. This greatly reduces bandwidth use.

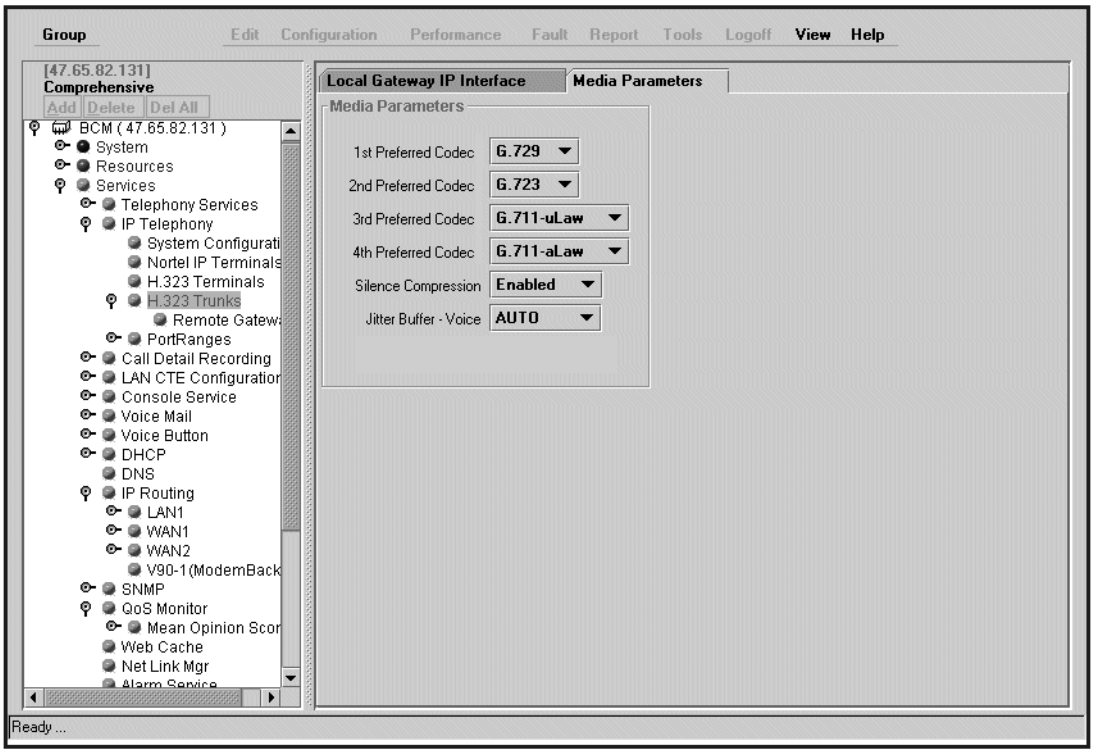
G.723.1 and G.729 support silence compression. If a conversation is using G.711, silence compression does not occur.

To set the silence compression:

1 In Unified Manager, open **Services**, **IP Telephony**, and click on **H.323 trunks**.

2 Click on the **Media Parameters** tab. The Media Parameters dialog appears:

Figure 19 Media Parameters



3 Click the **Silence Compression** drop-down menu, and select either **Enabled** or **Disabled**. If you select Enabled, silence compression is only used when a G.729 or G.723.1 codec is in use.

Setting Jitter Buffers

This section explains how to select the jitter buffer size used on VoIP trunks.

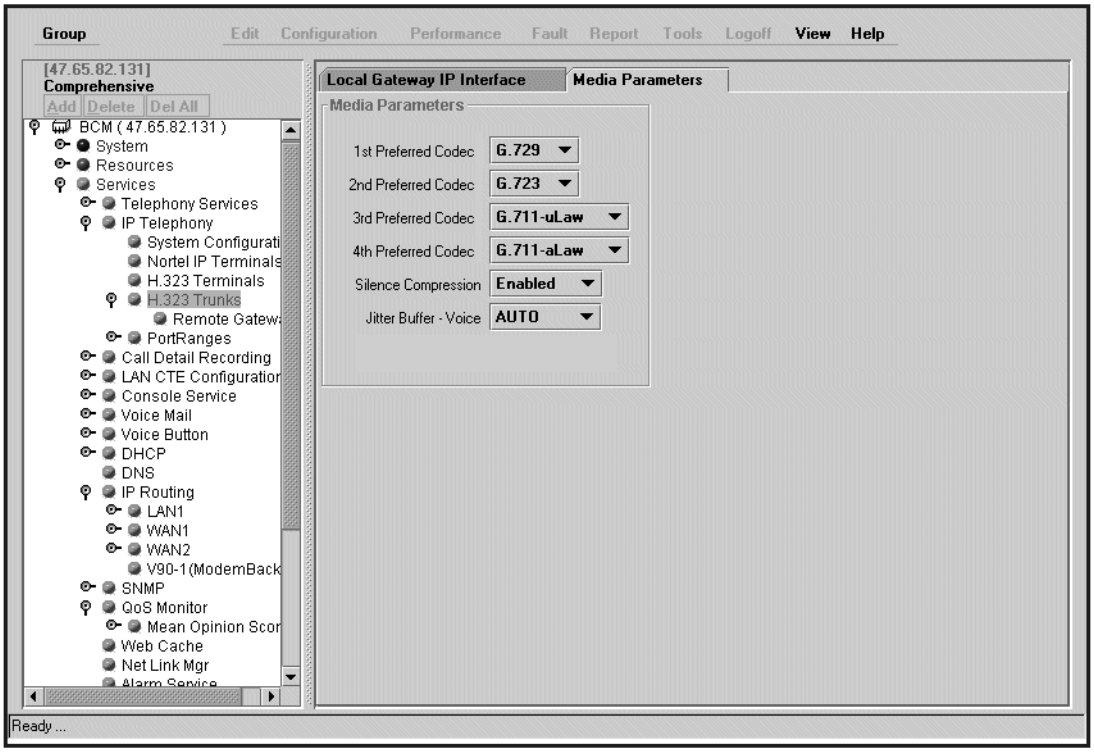
Jitter buffers are explained in detail in "Jitter Buffer" on page 24.

To set the jitter buffer size for VoIP trunks:

1 In Unified Manager, open **Services**, **IP Telephony**, and click on **H.323 trunks**.

2 Click on the **Media Parameters** tab. The Media Parameters dialog appears:

Figure 20 Media parameters



3 In the **Voice Jitter Buffer**, select a value.

Outgoing call configuration

This section explains how to set up your system to place calls through VoIP trunks. The system at the other end of the call must be set up to receive VoIP calls. For information on this, see "Incoming call configuration" on page 70.

Before telephones on the Business Communications Manager can use VoIP trunks services, the VoIP trunks must be placed in a line pool. Outgoing call configuration consists of the following steps:

- Putting VoIP lines into a line pool
- Configuring the access code for the line pool
- Configuring DNs to access the VoIP line pool
- Configuring a remote gateway
- Configuring PSTN fallback

Putting VoIP lines into a line pool

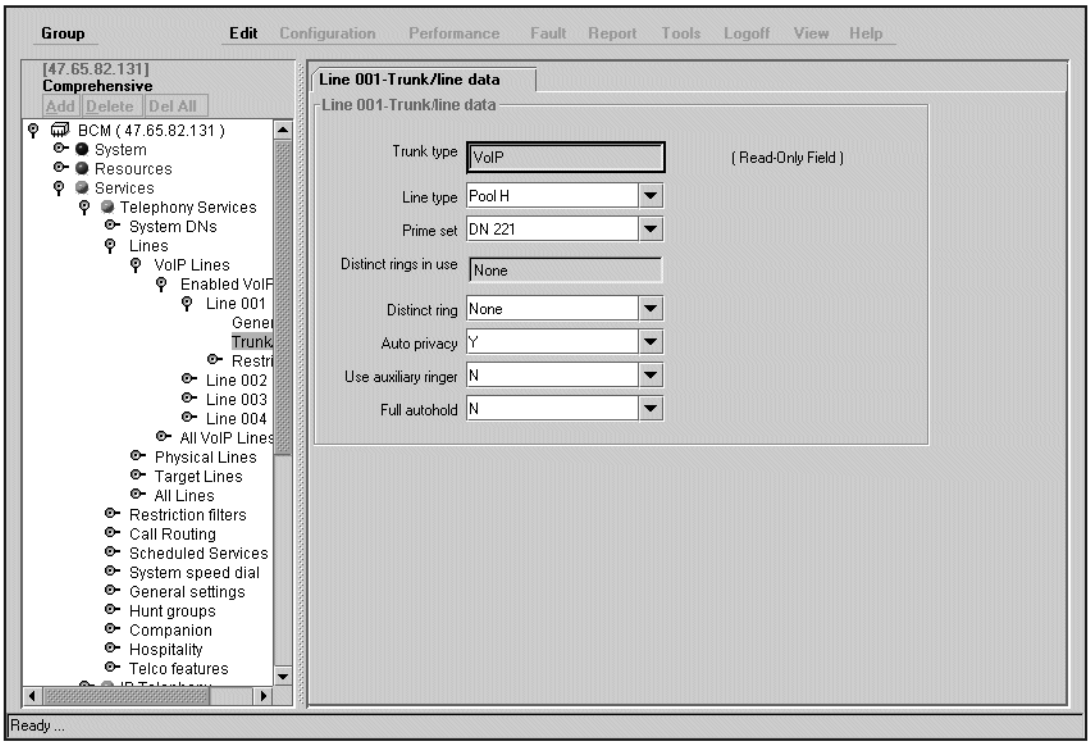
Lines 001 to 060 are reserved for VoIP trunks. However, they can be used only if you have entered the appropriate keycodes to activate them.

When putting VoIP trunks into a line pool, choose a line pool that is not used for any other type of line.

To put your lines into a line pool:

1 In Unified Manager, open **Services, Telephony Services**, **Lines**, **VoIP lines**, **Line 001**, and click on **Trunk/Line Data**. The Trunk/Line Data screen appears.

Figure 21 Trunk/Line data



2 In the **Line type** field, set a line pool that is not used by any non-VoIP lines.

Repeat this procedure for as many trunk lines as you have keycodes for. You can use the same line pool for all VoIP lines.

Configuring the Access code for the Line Pool

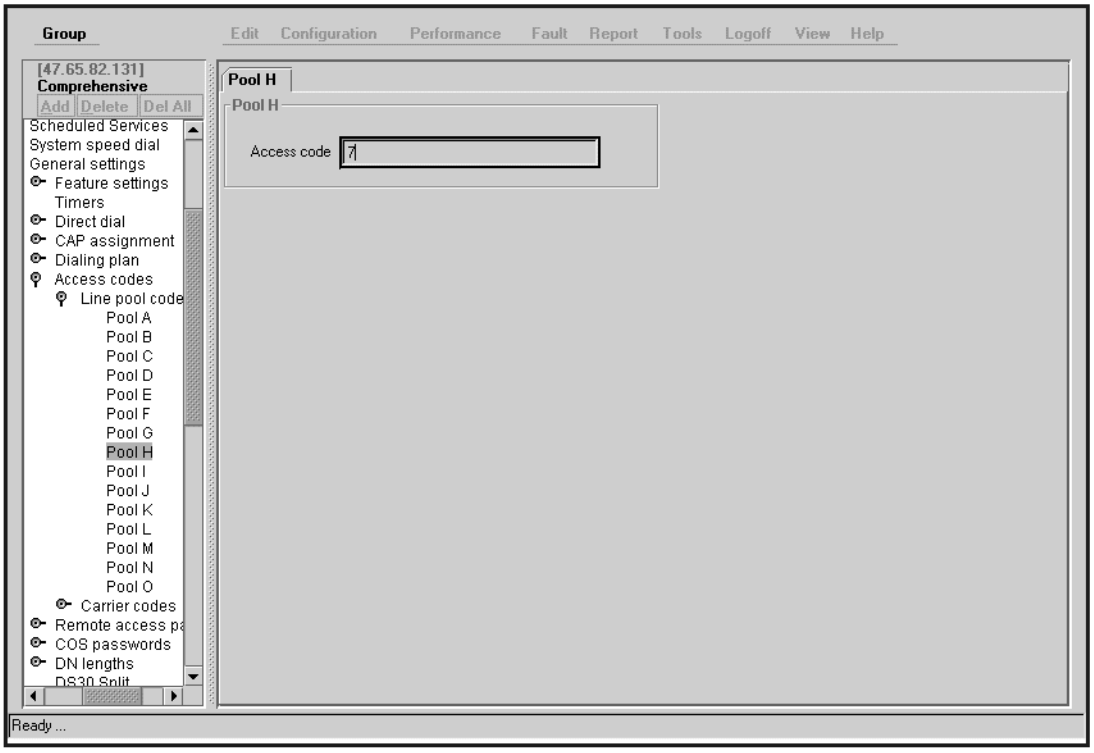
An access code is a number that users dial from their telephones to access the line pool containing VoIP trunks.

Note: Set up an access code for the line pool only if you are NOT planning to use PSTN fallback.

To set up access codes:

1 In Unified Manager, open **Telephony Services**, **General Settings**, **Access Codes**, **Line Pool Codes,** and click on the line pool that you selected as the VoIP line pool.
The Pool screen appears.

Figure 22 Line pool



2 Enter a unique access code for this line pool. Ensure that no other line pools use this access code.

Configuring DNs to access the VoIP line pool

Each DN that is to use the VoIP lines must be authorized to use the VoIP line pool:

1. In Unified Manager, open **Services**, **Telephony Services**, **System DNs, Assigned DNs**, **DN XXX**, **Line Access**, and click **Line Pool Access**. DN XXX is any DN that you want to allow to use VoIP trunking.
2. Click **Add**.The Add Line Pool Access dialog appears.
3. Type the letter of the VoIP line pool.
4. Click **Save**.

Repeat this procedure for every DN you want to allow to use VoIP trunks.

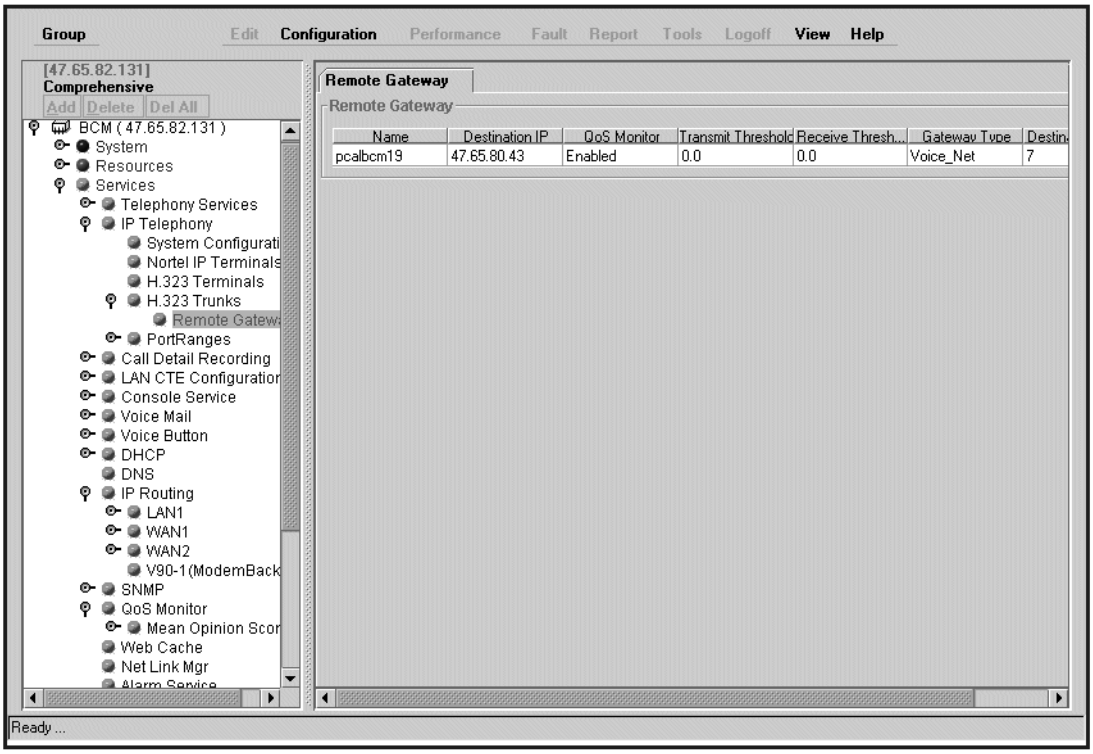
Configuring a remote gateway

This section explains how to configure the Business Communications Manager to communicate with other Business Communications Managers and/or other VoIP gateways such as Meridian ITG. The remote gateway list must contain an entry for every remote system to which you want to make VoIP calls.

To add an entry to the remote gateway list:

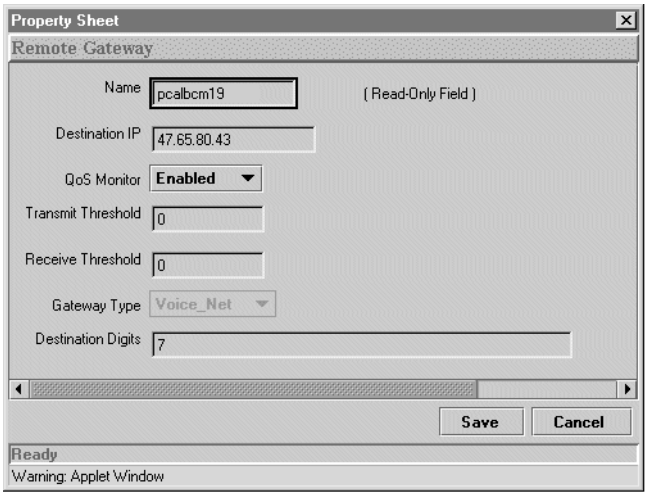
1. In Unified Manager, open **Services**, **IP Telephony**, **H.323 Trunks**, and click on **Remote Gateway**. The remote gateway tab appears.

Figure 23 Remote gateway list



2 In the **Configuration** menu, select **Add a new entry**. The Remote Gateway window appears

Figure 24 Remote gateway dialog



3 In the **Name** field, type a name for the remote system.

4 In the **Destination IP** field, enter the IP address of the system.

5 In the **Destination Digits** field, set the leading digits which callers can dial to route calls through the remote gateway. Ensure that there are no other remote gateways currently using this combination of destination digits. If multiple leading digits map to the same remote gateway, separate them with a space. For example, 7 81 9555.

6 Set the **QoS monitor** option. If you intend on using fallback to a PSTN line, set the QoS monitor to **enabled**. Otherwise, set it to **disabled**. For information on enabled QoS, see "Turning on QoS monitor" on page 68.

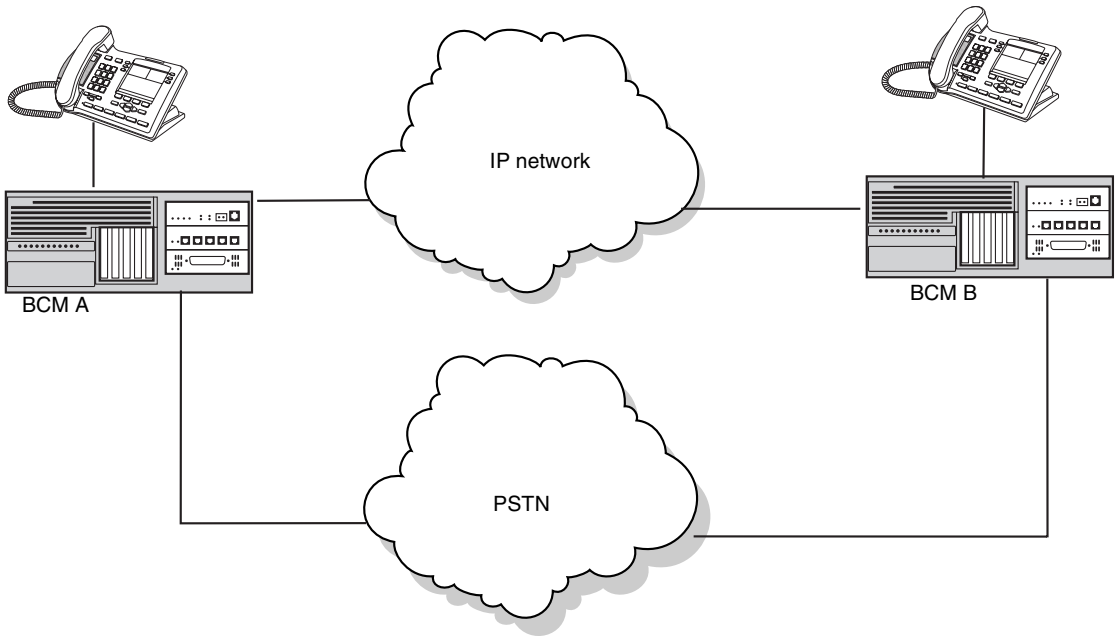
7 Click **Save**.

Configuring PSTN fallback

By enabling PSTN fallback, you allow the system to check the availability of suitable bandwidth for a VoIP call. If the bandwidth is adequate, it connects the call across the VoIP line. If the bandwidth is not adequate, it routes the call across the PSTN.

In a network configured for PSTN fallback, there are two connections between a Business Communications Manager and a remote system. One connection is a VoIP trunk, the other is a T1, BRI, PRI or analog line. When a user dials the destination code, the system checks first to see if the connection between the two systems can support an appropriate level of QoS. If it can, the call proceeds as normal. If the minimum acceptable level of QoS is not met, the call is routed over a different route, commonly a PSTN.

Figure 25 PSTN fallback diagram



Before configuring fallback, you must have both your VoIP trunk and your fallback line properly configured and line pools created for each. For information on creating a VoIP line pool, see "Putting VoIP lines into a line pool" on page 57. You create a PSTN line pool in the same manner. Ensure that you use a different line pool for PSTN lines than for VoIP lines.

Setting up PSTN fallback includes:

- Setting up a VoIP schedule
- Configuring routes
- Creating a destination code
- Configuring digits
- Activating the VoIP schedule
- Turning on QoS monitor

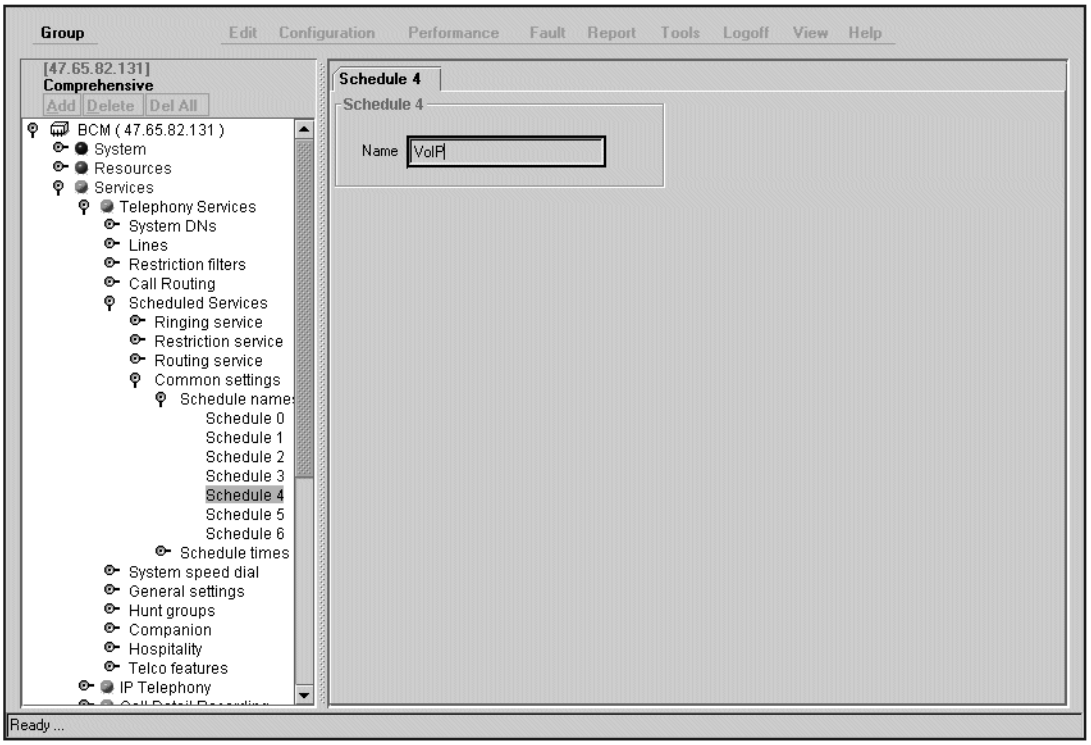
Setting up a VoIP schedule

Setting up a VoIP schedule allows you to create two different call routes for a single destination code. One of these is a VoIP route. The other is typically a PSTN route. The PSTN route uses the 'Normal' schedule which runs when no other schedule is activated.

To set up the VoIP route:

1 In the Unified Manager, open **Services**, **Telephony Services**, **Scheduled Services**, **Common Settings**, **Schedule Names:**

Figure 26 VoIP schedule

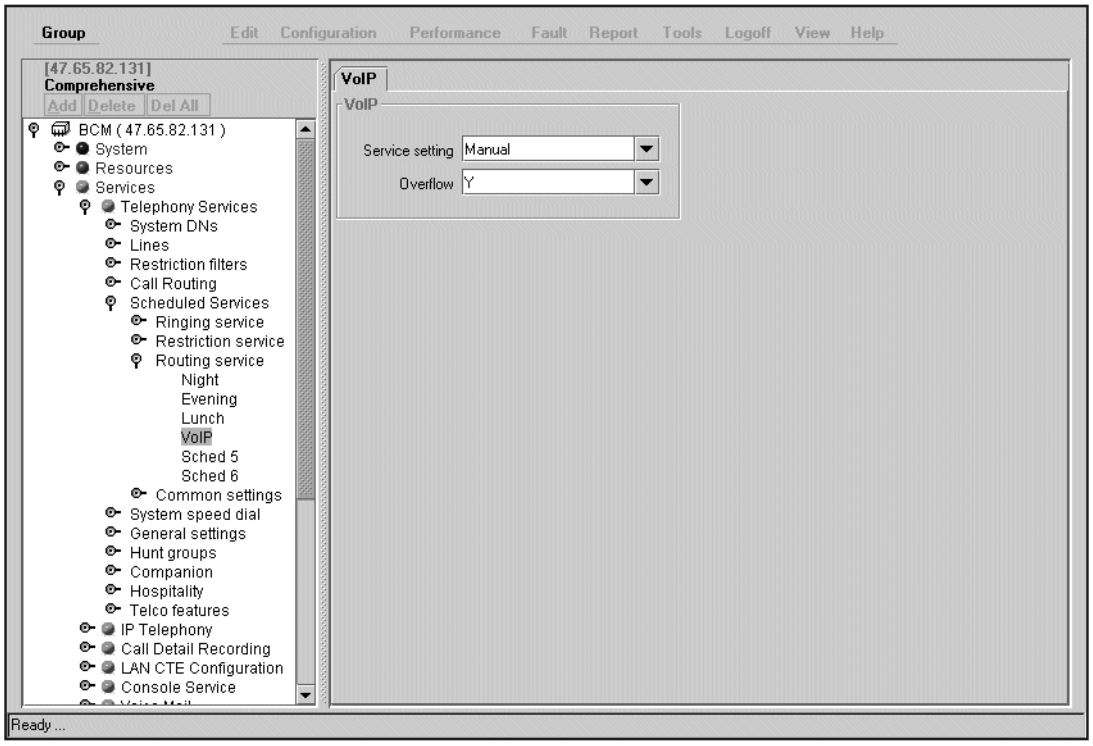


2 Select a schedule that will not be used for another purpose, typically Schedule 4.

3 Change the schedule name to **VoIP**.

4 Open **Services**, **Telephony Services**, **Scheduled Services**, **Routing Service**, and click on **VoIP**.

Figure 27 VoIP Routing Service



5 Change the **Service** setting to **Manual**.

6 Change the **Overflow** setting to **Y**.

Configuring routes

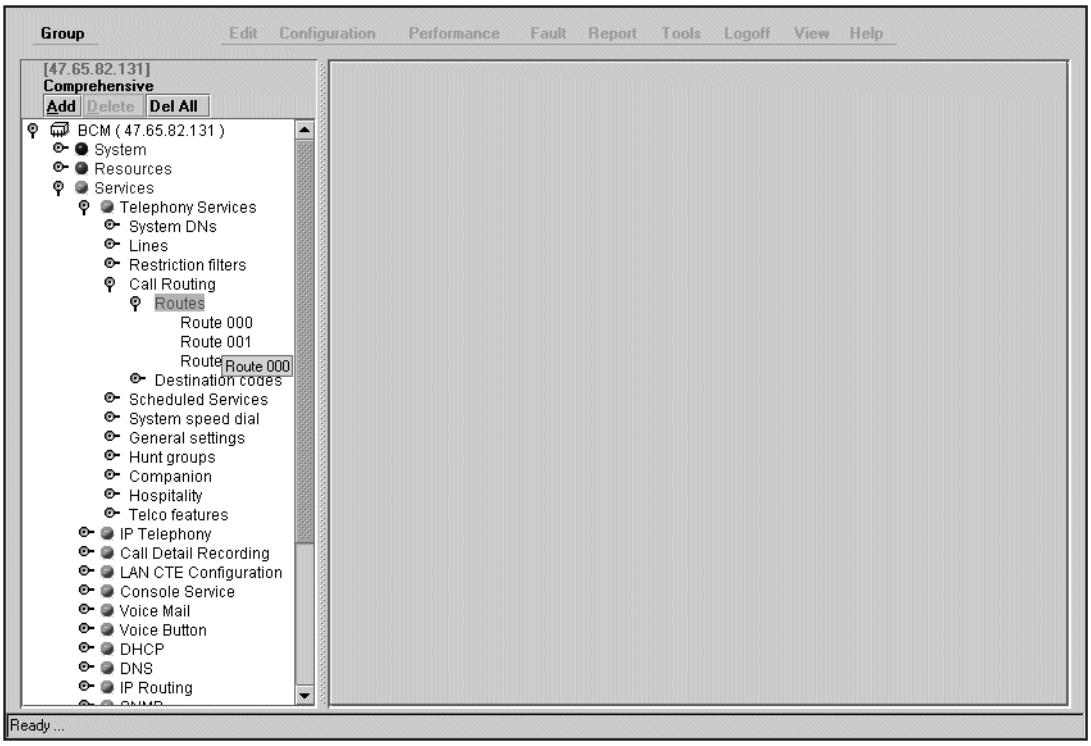
Configuring routes allows you to set up access to the VoIP and the PSTN line pools. These routes can be assigned to destination codes using schedules.You must configure your PSTN and VoIP line pools before continuing.

Note: If you already have routes for your PSTN or VoIP line pools configured, you do not need to configure new routes, unless you cannot match the dialed digits. See "Configuring digits" on page 67.

To configure the PSTN route:

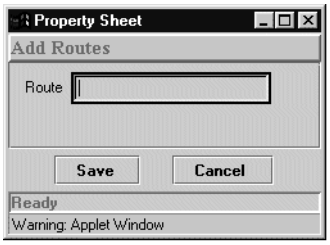
1 Open **Services**, **Telephony Services**, **Call Routing** and click on **Routes**.

Figure 28 Route list



2 Click the **Add** button. The Add Routes dialog appears.

Figure 29 Add route dialog



3 Type a number between 001 and 999 to define this route. Only numbers not otherwise assigned will be allowed by the system.

4 Click the route you just created.

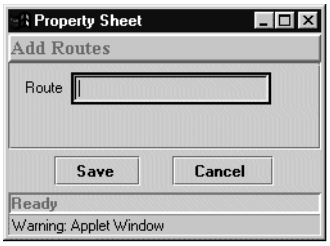
5 In the **Use Pool** box, type the letter of the line pool for the fallback lines.

To configure the VoIP route:

1 Open **Services**, **Telephony Services**, **Call Routing** and click on **Routes**.

2 Click the **Add** button. The Add Routes dialog appears.

Figure 30 Add route dialog



3 Type a number between 001 and 999 to define this route.Only numbers not otherwise assigned will be allowed by the system.

4 Click the route you just created.

5 In the **Use Pool** field, type the letter of the line pool for the VoIP lines.

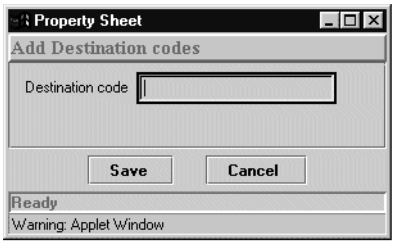
Creating a destination code

Creating a destination code allows you to combine the two routes created in "Configuring routes" on page 63 under a single dialed code. When this code is dialed, the Business Communications Manager will select the VoIP line if possible, and if not, will fall back to the PSTN line.

1 Open **Services**, **Telephony Services**, **Call Routing** and highlight **Destination Codes**.

2 Click **Add**. The Destination Code dialog appears.

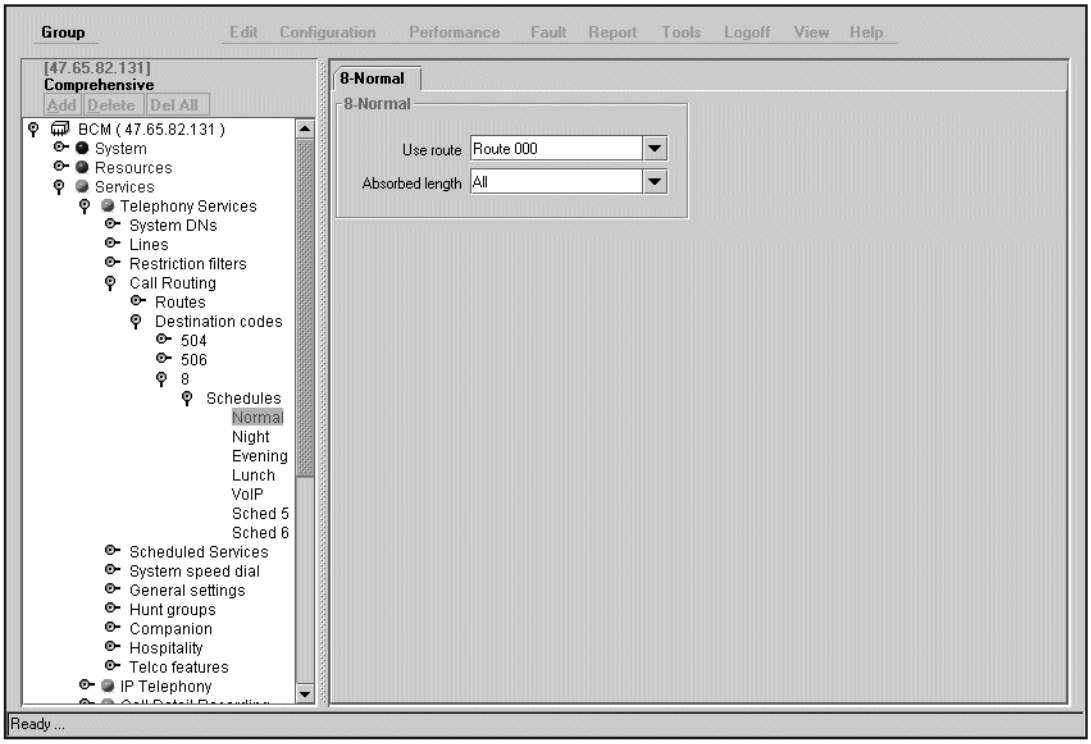
Figure 31 Add destination code dialog



3 Type a digit for this destination code and click **Save**.

4 Click on the destination code you just created, click on the key beside **Schedules**, and click **Normal**.

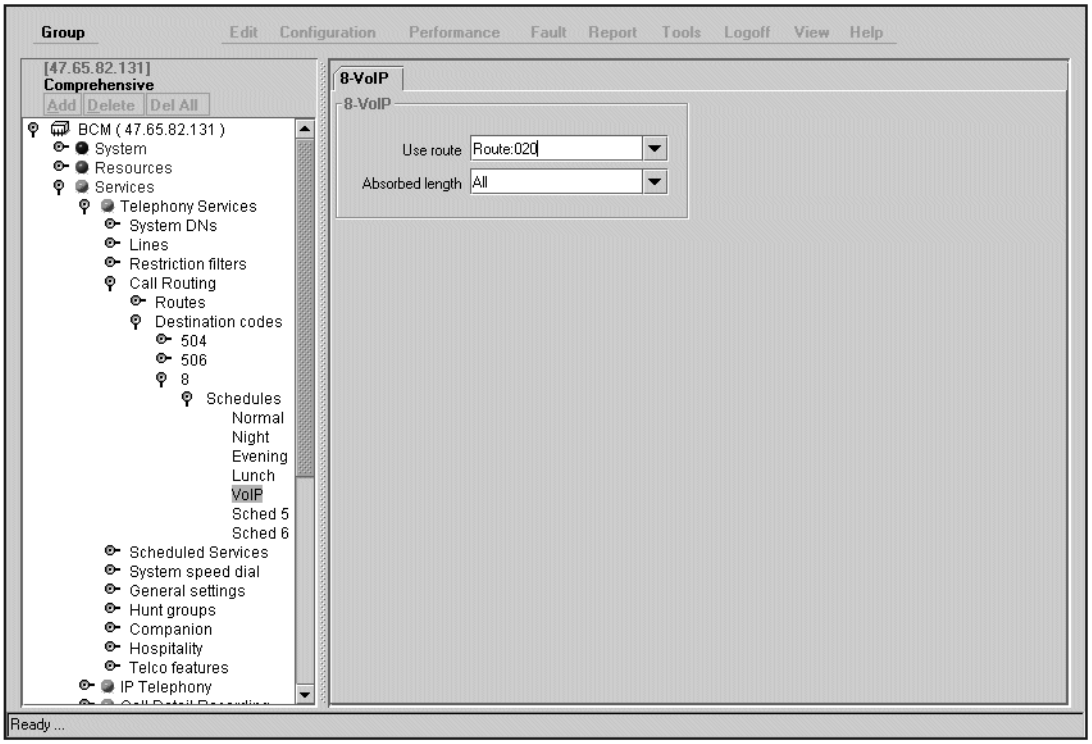
Figure 32 Normal schedule



5 Change **Use Route** to the route you configured for your PSTN fallback line.

6 Under the **Schedules** list, highlight **VoIP**.

Figure 33 VoIP schedule



7 Change **Use Route** to the route you configured for your VoIP line.

Configuring digits

For PSTN fallback to work, you must ensure that the digits the user dials will be the same regardless of whether the call is going over the VoIP trunk or the PSTN. In many cases, this involves configuring the system to add (inserting) or remove (absorbing) digits. For information of inserting and absorbing digits, see the *Business Communications Manager 2.5 Programming Operations Guide*.

For example: a caller dials 7 to access the VoIP line, 55 to select the remote gateway, and then 224 to dial a DN on the remote Business Communications Manager. The dialing plan must be set up so that calls are treated the same way by the VoIP and PSTN routes. In the example above, dialing 755224 must access the same DN even if the call is routed across the PSTN and not through VoIP.

Activating the VoIP schedule

Before activating the VoIP schedule, calls using the destination code are routed over the PSTN. This is because the system is set to use the ‘Normal’ schedule, which routes the call over the PSTN.

Once the VoIP schedule is activated, calls are routed over the VoIP trunk.

The VoIP line must be activated from the control set for the schedule. For information about control sets, see the *Business Communications Manager 2.5 Programming Operations Guide*.

To activate the VoIP lines:

1. Dial Feature 873 from the control set for the VoIP trunk. The phone prompts you for a password.
2. Type the password. Press OK. The first schedule appears.
3. Scroll down the list until VoIP is selected.

Press OK.

The VoIP schedule stays active even after a system reboot, and can only be deactivated manually.

To deactivate the VoIP line:

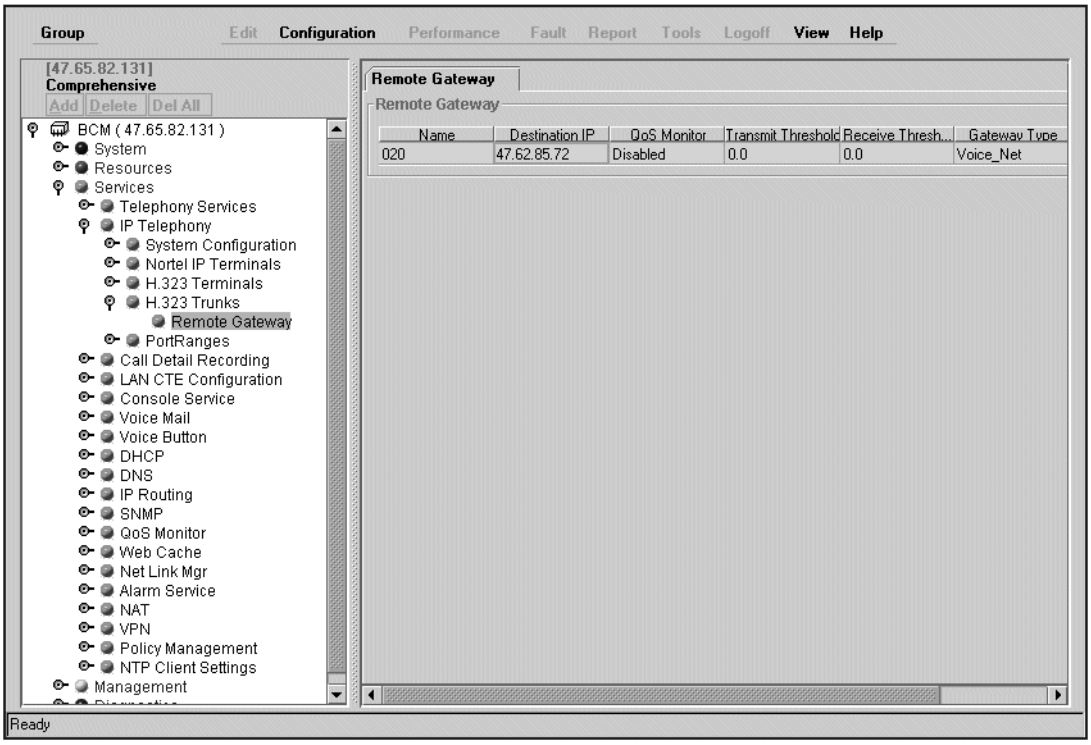
1. Dial Feature # 873. The phone prompts you for a password.
2. Type the password. Press **OK**. The system restores Normal schedule.

Turning on QoS monitor

For fallback to function, the QoS monitor must be enabled:

1. In Unified Manager, open **Services**, **IP Telephony**, **H.323 Trunks**, and click on **Remote Gateways**:

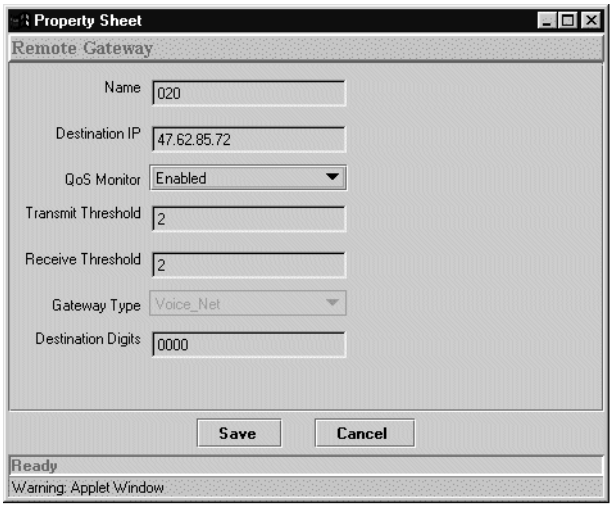
Figure 34 Remote Gateway list



2 Select the Remote Gateway for which you want to enable QoS Monitoring.

3 From the **Configuration** menu, click **Modify Entry**.

Figure 35 Remote Gateway dialog



4 For the **QoS Monitor** field, select **Enabled**.

5 Set the **Transmit Threshold** and **Receive Threshold** to a value between 0 and 5. This marks the level of quality that the gateway must be able to support before transmitting a call. In most cases, the transmit threshold and receive threshold should be the same. On a line where

communications in one direction are more important than in the other direction, you can set up asymmetrical thresholds.

For information about using the QoS monitor, see "Quality of Service Monitor" on page 77.

Enabling PSTN fallback

To enable PSTN fallback:

1. Open **Services**, **IP Telephony** and click on **H.323 trunks**.
2. Click the **Fallback to Circuit-Switched** menu and select **Enabled-All** or **Enabled-TDM-only**. Enabled-TDM-only enables fallback for calls originating on TDM telephones. This is useful if your IP telephones are connected remotely, on the public side of the Business Communications Manager network, because PSTN fallback is unlikely to result in better quality of service in that scenario.

Incoming call configuration

This section explains how to receive incoming calls placed over a VoIP network. For information about setting up your Business Communications Manager to place outgoing VoIP calls, see "Outgoing call configuration" on page 56.

Assign a target line to the DN

A target line routes incoming calls to specific telephones (DNs) depending on the incoming digits. This process is independent of the trunk over which the call comes in. The mapping of the target lines involves two steps:

- The incoming digits (e.g. 321) are mapped to a target line (e.g. 241) by setting the Received Number to the incoming digits (e.g. to line 241 to 321).
- The target line is mapped to a telephone by assigning the line (241) to the telephone.

For a detailed explanation of target lines, see the *Business Communications Manager 2.5 Programming Operations Guide*.

To assign a target line to a DN:

1. In Unified Manager, open **Services/Telephony Services/System DNs/Active Set DNs**.
2. Choose the DN of the telephone where you want the line to be directed.
3. Choose **Line Access/Line assignment** and click the **Add** button.
4. Enter the number of an available target line (241-412). Click the **Save** button.
5. Click on the line number you just created. The DN/Line screen appears in the right frame.
6. Ensure that **Appearance type** is set to **Appr & Ring**.
7. Go to **Services/Telephony Services/Lines/Target Line/**<Target line number from step 4>.

8 Click the key beside **Trunk/line data**.

9 Click on **Received number**.

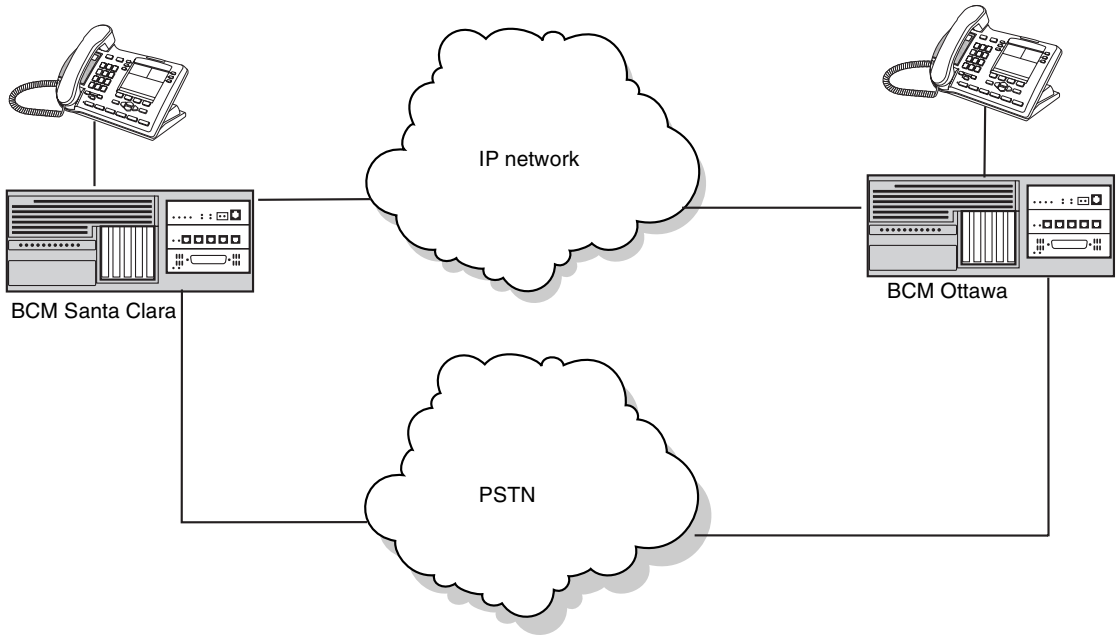
10 In the **Public number** field, enter the DN.

The telephone assigned to that DN can now receive calls routed across VoIP trunks.

Example configuration

This section walks through a sample Business Communications Manager configuration. In this scenario, two Business Communications Managers in different cities are connected to a WAN. One Business Communications Manager resides in Ottawa; the other in Santa Clara. The systems already communicate through a PRI line, which will be configured to be used for fallback. Both systems already have all keycodes installed for eight VoIP lines, and resources properly allocated for VoIP trunking. For information about keycodes, see the *Business Communications Manager 2.5 Keycode Installation Guide*. For information on Resource Allocation, see *Configuring the MSC Resources* in the *Business Communications Manager 2.5 Programming Operations Guide.*

Figure 36 Example PSTN fallback



Business Communications Manager Ottawa

- Private IP address: 10.10.4.1
- Public IP address: 47.62.54.1
- Phones 221-231
- From this system, dial 9 to get onto PSTN

Business Communications Manager Santa Clara

- Private IP address: 10.10.5.1
- Public IP address: 47.62.84.1
- Phones 321-331
- From this system, dial 9 to get onto PSTN

On Business Communications Manager Ottawa

This procedure details actions that the installer performs to set up the Business Communications Manager Ottawa.

1. The installer obtains keycodes for eight VoIP lines, and inputs the keycodes into the system. Each Business Communications Manager has 10 phones, VoIP lines are available for eight phones, but if all 10 phones try to place or receive VoIP calls at the same time, two of the calls will be rerouted to the PSTN. The installer sets up 221 as the Control set for each line, so that the VoIP schedule can be manually activated. This setup is necessary for PSTN fallback.
2. The installer sets the published IP address.
   Because the public IP network is connected to the LAN 2 connection, the installer sets the published IP address to LAN 2. This is the address that devices on the Packet Data Network (PDN) will use to locate the system.
3. The installer configures the media for the system, using the following settings:
   - The first preferred codec is set to G.729. The installer chooses this setting due to the unique requirements of this installation.
   - Silence Compression is turned on.
   - Jitter Buffer is set to medium.
4. The installer puts eight VoIP lines into line pool O. Any line pool can be used as long as all of the lines in the pool are VoIP. The installer does not set an access code for the line pool, because the access code does not work with fallback. Instead, the line pool will be accessed using destination digits after the installer sets up PSTN fallback.
5. For each telephone on the system (DNs 221 to 231), the installer gives the DN access to line pool O.
6. The installer sets up a remote gateway for the Santa Clara Business Communications Manager, using the following settings:
   - Destination IP: **47.62.84.1** This is the published IP address of the Santa Clara Business Communications Manager.
   - QoS Monitor: **Enabled** This must be enabled for PSTN fallback to function.
   - Transmit Threshold: **3.0** This is a Mean Opinion Score (MOS) value that ensures that the VoIP lines are used as long as the system can provide moderate quality.
   - Receive Threshold: **3.0** This is a MOS value that ensures that the VoIP lines are used as long as the system can provide moderate quality.
   - Destination Digits: **44** This means that callers dial ‘44’ to call phones on the Santa Clara Business Communications Manager after dialing the destination digit.
7. The installer sets up a schedule called VoIP with these settings:

- Service: Manual
- Overflow: Y

8 The installer defines a new route called Route 003, and sets it to use line pool PRI-A.

9 The installer defines a new route called Route 100, and sets it to use line pool O. This is the line pool that contains the VoIP lines.

10 The installer creates a destination code of 7.

- Under the Normal schedule, the installer assigns Route 003, which uses line pool PRI-A.
- Under the VoIP schedule the installer assigns Route 100, which uses the VoIP lines in line pool O.

11 The installer configures the call digits. They must be configured so that calls will still be processed correctly if routed over PSTN. For information about configuring dialing plans, see the *Business Communications Manager 2.5 Programming Operations Guide*.

12 From the control set 221, the installer dials Feature 873 and selects the VoIP schedule. VoIP is now activated. At this point, the system is configured to make outgoing calls, but it is not set up to receive incoming calls.

13 The installer programs target line 241 with the received digits 221, then assigns this target line to DN 221. This means that calls received containing the digits 221 are delivered to DN 221. The installer repeats this procedure for each DN, using different received digits and target lines.

The Ottawa Business Communications Manager is now set to handle calls sent to and from a remote VoIP gateway. However, the Santa Clara Business Communications Manager must be set up before any calls can be made.

On Business Communications Manager Santa Clara

This procedure details actions that the installer performs to set up the Business Communications Manager Santa Clara.

1 The installer obtains keycodes for eight VoIP lines, and inputs the keycodes into the system. The installer sets up 321 as the Control set for each line, so that theVoIP route can be manually activated.

2 The installer sets the published IP address. Because the public data network (PDN) is connected to the LAN 2 connection, the installer sets the published IP address to LAN 2. This is the address that devices on the PDN will use to locate the system.

3 The installer configures the media for the system, using the following settings:

- The first preferred codec is set to G.729.
- Silence Compression is turned on.
- Jitter Buffer is set to medium.

4 The installer puts the first eight VoIP lines into line pool O. Any line pool can be used as long as all of the lines in the pool are VoIP. The installer does not set an access code for the line

pool, because the access code would not work with fallback. Instead, the line pool will be accessed using destination digits after the installer sets up PSTN fallback.

5 For each set on the system (DNs 321 to 331), the installer gives the set access to line pool O.

6 The installer sets up a remote gateway for the Santa Clara Business Communications Manager, using the following settings:

- Destination IP: 47.62.54.1 This is the published IP address of the Ottawa Business Communications Manager.
- QoS Monitor: Enabled This must be enabled for PSTN fallback to function.
- Transmit Threshold: 3.0 This is a MOS value that ensures that the VoIP lines are used as long as the system can provide moderate quality.
- Receive Threshold: 3.0 This is a MOS value that ensures that the VoIP lines are used as long as the system can provide moderate quality.
- Destination Digits: 55 This means that callers dial 55 to call phones on the Ottawa Business Communications Manager after dialing the destination digit.

7 The installer sets up a schedule called VoIP with these settings:

- Service: Manual
- Overflow: Y

8 The installer defines a new route called Route 003, and sets it to use PRI-A.

9 The installer defines a new route called Route 100, and sets it to use line pool O. This is the line pool that contains the VoIP lines.

10 The installer creates a destination code of 7.

- Under the Normal schedule, the installer assigns Route 003, which uses PRI-A.
- Under the VoIP schedule the installer assigns Route 100, which uses the VoIP lines in line pool O.

11 The installer configures the call digits. They must be configured so that calls will still be processed correctly if routed over PSTN. For information about configuring dialing plans, see the *Business Communications Manager 2.5 Programming Operations Guide*.

12 The installer dials Feature 873 and selects the VoIP schedule. VoIP is now activated. At this point, the system is configured to make outgoing calls, but it is not set up to receive incoming calls.

13 The installer programs target line 241 with the received digits 321, then assigns this target line to DN 321. This means that calls received containing the digits 321 are delivered to DN 321. The installer repeats this procedure for each telephone using different received digits and target lines.

Making calls

From a set on Business Communications Manager Ottawa, a caller dialling a set on Business Communications Manager Santa Clara must dial the destination code, the destination digits for the Business Communications Manager Santa Clara remote gateway and the DN of the set. For example, dialing 744322 would connect as follows:

- 7 is the destination code. If a suitable level of QoS is available, the call is routed through the VoIP trunks.
- 44 is the remote gateway. The call is sent across the PDN using the IP address of the Santa Clara Business Communications Manager.
- 322 is linked to the target line associated with DN 322. The call arrives at the phone with the DN 322.

If a user in Santa Clara wanted to make a local call in Ottawa, they would dial 7559 followed by the local Ottawa number. The digit 7 accesses the VoIP line pool and 55 accesses the Ottawa Business Communications Manager, while 9 accesses an Ottawa outside line.

Connecting an i200X telephone

This section takes the example above and uses it to demonstrate how an installer would configure an i2004 phone on the system. For information on configuring i200X telephones, see Chapter 3, "Installing IP Telephones," on page 31.

Note: IP clients require an IP network to reach the Business Communications Manager. However, they do not need to use VoIP trunks to communicate beyond the Business Communications Manager. They can use any type of trunk, just as any other phone on the Business Communications Manager can.

Connecting an i200X telephone on the LAN

In this case, the Santa Clara administrator wants to connect an i2004 phone using the LAN 1 network interface.

1. The installer sets up the Business Communications Manager to handle IP telephone by turning Registration to ON, and Auto Assign DNs to ON.
2. The installer connects the telephone to the LAN, and sets it up using the following settings:
   - Set IP address:10.10.5.10
   - Default GW: 10.10.5.1 This is the IP address of the default gateway on the network, which is the nearest router to the telephone.
   - S1 IP address: 47.62.84.1 This is the published IP address of the Business Communications Manager.
3. The Business Communications Manager automatically assigns the telephone the DN of 348.
4. The installer sets up a target line for DN 348, using the Received Digits 348.

This phone would follow all of the same dialing rules as the other telephones on the Santa Clara Business Communications Manager. A caller could dial 321 to connect with telephone 321, dial 9 to access the PSTN, or dial 755241 to access a telephone on the Ottawa system.

Configuring NetMeeting clients

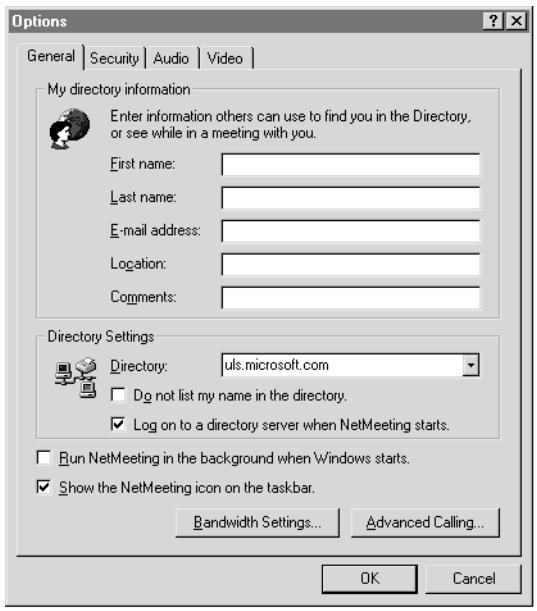
NetMeeting is an application available from Microsoft which uses the H.323 protocol.

To use NetMeeting:

1 Install NetMeeting on the client computer.

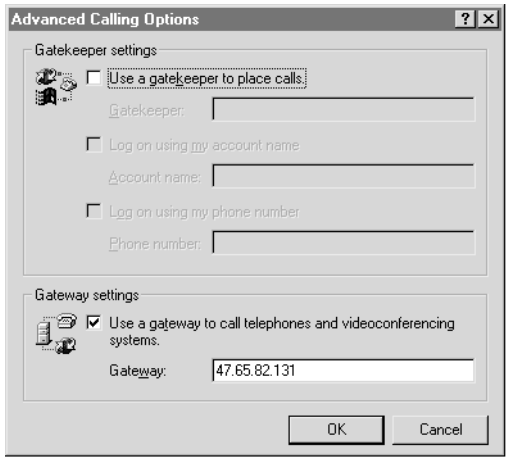
2 In the **Tools** menu, click **Options**. The options dialog appears.

Figure 37 NetMeeting options



3 Click **Advanced Settings**. The advanced settings dialog appears.

Figure 38 NetMeeting advanced options



4 Under **Gateway** settings, select the **Use a gateway...** option. In the **Gateway** field, type the published IP address of the Business Communications Manager.

5 Add a remote gateway to your system as explained in "Configuring a remote gateway" on page 59. When prompted for the IP address of the remote gateway, type the IP address of the client computer.

Repeat this procedure for every NetMeeting client you want to set up.

Quality of Service Monitor

The Quality of Service Monitor is an application that monitors the quality of the IP channels. It does this by performing a check every 15 seconds. The QoS Monitor determines the quality of the intranet based on threshold tables for each codec. If the QoS Monitor is enabled, and it determines that the quality of service falls below the set threshold, it will trigger fallback to PSTN. For information about setting up the system to use QoS and fallback to PSTN, see "Configuring PSTN fallback" on page 60.

Quality of Service Status

The QoS Status displays the current network quality described as a Mean Opinion Score (MOS) for each IP destination. A pull-down menu allows the administrator to view the MOS mapping. Table 9 shows a sample QoS Monitor.

Table 9 QoS status

IP	QoS Monitor	G.729		G.711		G.723.1 6.3 kbit/s		G.723.1 5.3 kbit/s	
		Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx
47.192.5.2	Enabled	4.50	4.50	4.00	4.30	4.75	4.70	4.80	4.90
47.192.5.6	Disabled	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Note: For the QoS monitor and PSTN fallback to function, both Business Communications Managers must list each other as a Remote Gateway and QoS Monitor must be enabled on both systems.

Updating the QoS Monitor data

To update the table with the most current values:

From the **View** menu, select **Refresh**.

Port settings

In some installations, you may need to adjust the port settings for the Business Communications Manager can work with other devices.

Using firewalls

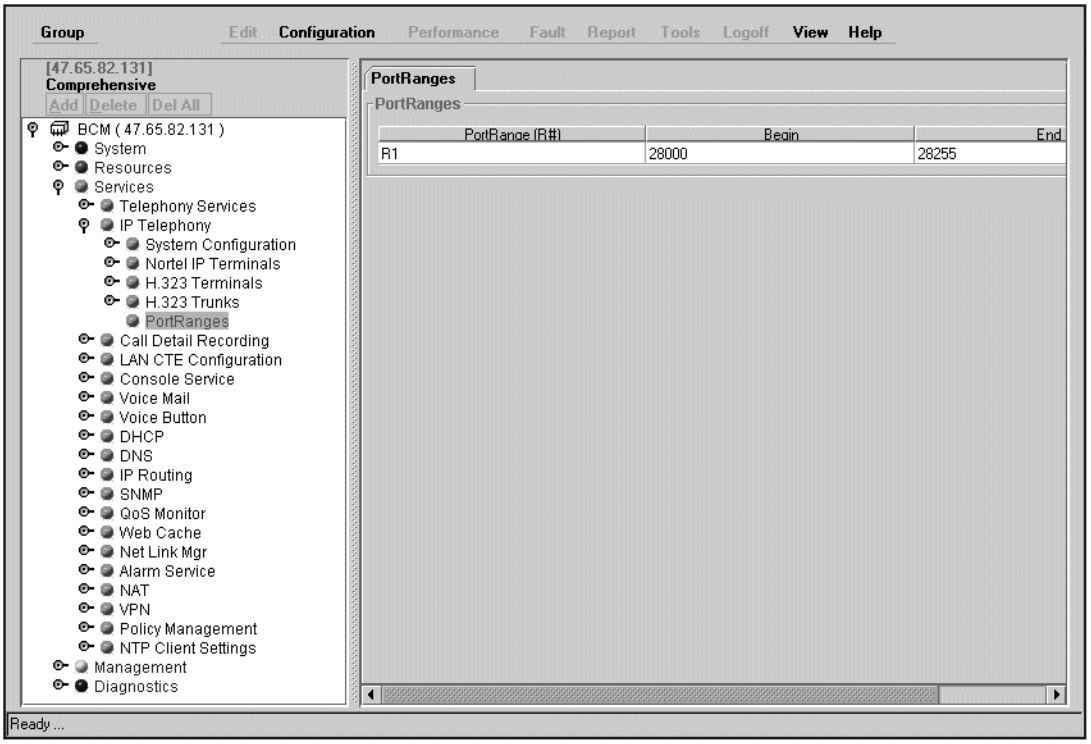
Firewalls can interfere with communications between the Business Communications Manager and another device. The port settings must be properly configured for VoIP communications to function properly. Using the instructions provided with your firewall, ensure that communications using the ports specified for VoIP are allowed.

An i2004 telephone uses ports between 51000 and 51200 to communicate with the Business Communications Manager.

The Business Communications Manager by default uses ports 28000 to 28255 to transmit VoIP packets. To modify these settings:

1 In Unified Manager, open **Services**, **IP Telephony**, **Port Ranges**.

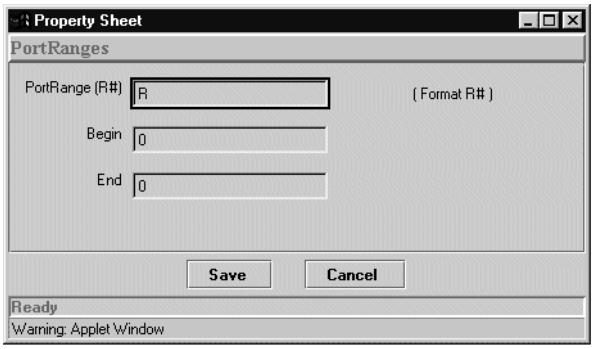
Figure 39 Port Ranges



2 Select the **Port Range** you want to modify.

3 From the **Configure** menu, select **Modify PortRanges**. The Modify PortRanges dialog appears.

Figure 40 Port ranges dialog



4 Change the port settings.

5 Click the **Save** button.

Port settings for legacy networks

Business Communications Manager 2.5 uses UDP port ranges to provide high priority to VoIP packets in existing legacy IP networks. You must reserve these same port ranges and set them to high priority on all routers that an administrator expects to have QoS support. You do not need to reserve port ranges on DiffServ networks.

You can select any port ranges that are not used by well-known protocols or applications.

Each H.323 or VoIP Realtime Transfer Protocol (RTP) flow uses two ports for each direction. The total number of UDP port numbers to be reserved depends on how many concurrent RTP flows are expected to cross a router interface. In general:

- Backbone routers reserve more ports than edge routers.
- The port ranges on edge routers are a subset of the backbone router port ranges.
- Include port number UDP 5000 in the reserved port ranges, for the QoS monitor.
- The port ranges reserved in a Business Communications Manager 2.5 system are also reserved by the remote router.
- You must reserve two ports for each voice call you expect to carry over the WAN link.
- You can reserve multiple discontinuous ranges. Business Communications Manager 2.5 requires that each range meet the following conditions:
  - Each range must start with an even number.
  - Each range must end with an odd number.
  - You cannot have a total of more than 256 ports reserved.

Using a gatekeeper

The Business Communications Manager supports the use of an ITU-H323 gatekeeper. A gatekeeper is a third-party software application residing somewhere on the network, which provides services such as:

- address translation
- admission control (ARQ)
- bandwidth control
- zone management

H.323 endpoints such as the Business Communications Manager are configured with one or more alias names that are registered with the gatekeeper. The gatekeeper stores the alias-IP mapping internally and uses them to provide alias to IP address translation services. Later if an endpoint's IP address changes, that endpoint has to re-register it with the gatekeeper.

See the gatekeeper software documentation for information about changing IP addresses.

The call signalling method

The call signalling method defines how the Business Communications Manager prefers call signalling information to be directed. Call signaling establishes and disconnects a call. The Business Communications Manager can use three types of call signalling:

- **Direct**: Under the direct call signalling method, call signalling information is passed directly between endpoints. The remote gateway table in the Unified Manager contains a mapping of phone numbers which the Business Communications Manager uses to perform DN to IP address resolution.
- **Gatekeeper Resolved**: Gatekeeper Resolved signalling uses a gatekeeper for call permission and address resolution. All call signalling occurs directly between H.323 endpoints. In effect, the gateway requests that the gatekeeper resolves the phone numbers into IP addresses, but the gatekeeper is not involved in call signalling.
- **Gatekeeper Routed**: Gatekeeper Routed signalling uses a gatekeeper for call permission and address resolution. In this method, call signalling is directed through the gatekeeper.

For information on changing the call signalling method, see "Alias names" on page 80.

Note: The Business Communications Manager can request a method for call signaling, but whether this request is granted depends on the configuration of the gatekeeper. Ultimately, the gatekeeper decides which call signalling method to use.

Alias names

One or more alias names may be configured for a Business Communications Manager. Alias names are comma delimited, and may be one of the following types:

- **E.164** — numeric identifier containing a digit in the range 0-9 (commonly used since it fits into dialing plans). Identified by the keyword "TEL:"
- **H323Identifier** — alphanumeric strings representing names, e-mail addresses, etc. Identified by the keyword "NAME:"
- **Transport Address** — IP Address. Identified by the keyword "TA:"

In the following example the Business Communications Manager is assigned an E.164 and an H323 Identifier alias:

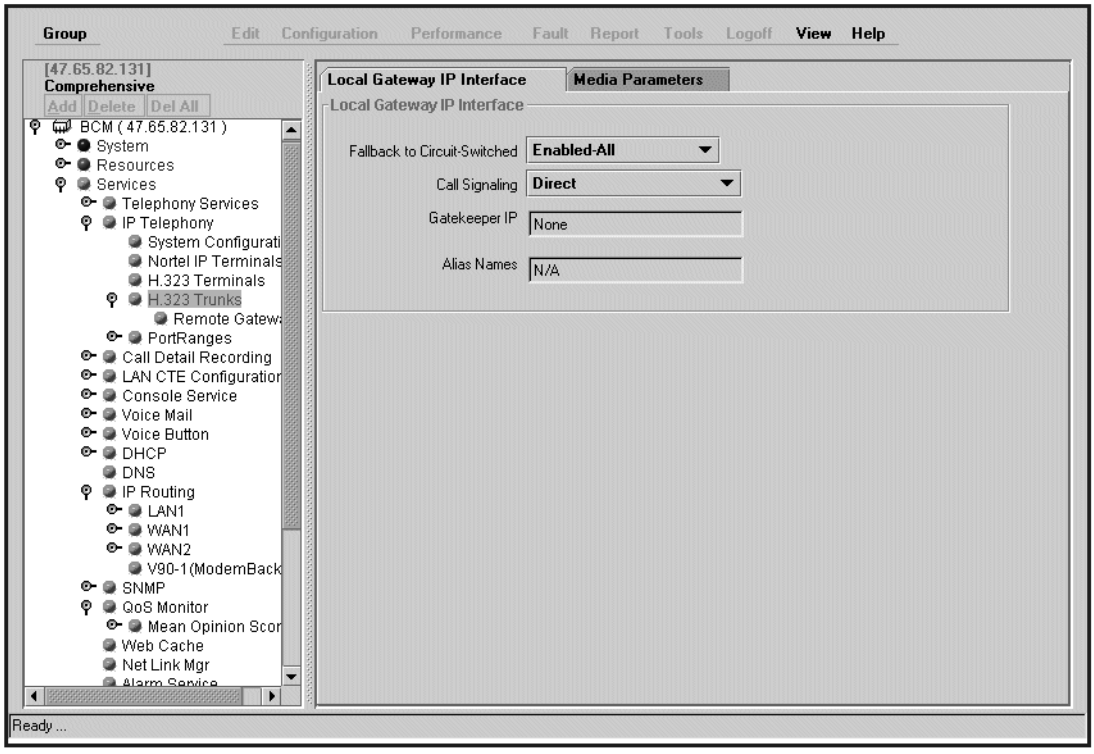
```
Alias Names: tel:76, name:bcm10.nortel.com
```

Modifying the call signalling method

To modify the call signalling method:

1 In the Unified Manager, open **Services**, **IP Telephony**, and click on **H.323 trunks**:

Figure 41 Local gateway IP interface



2 In the **Call Signalling** list, select the appropriate setting. For information about the settings, see "The call signalling method" on page 80.

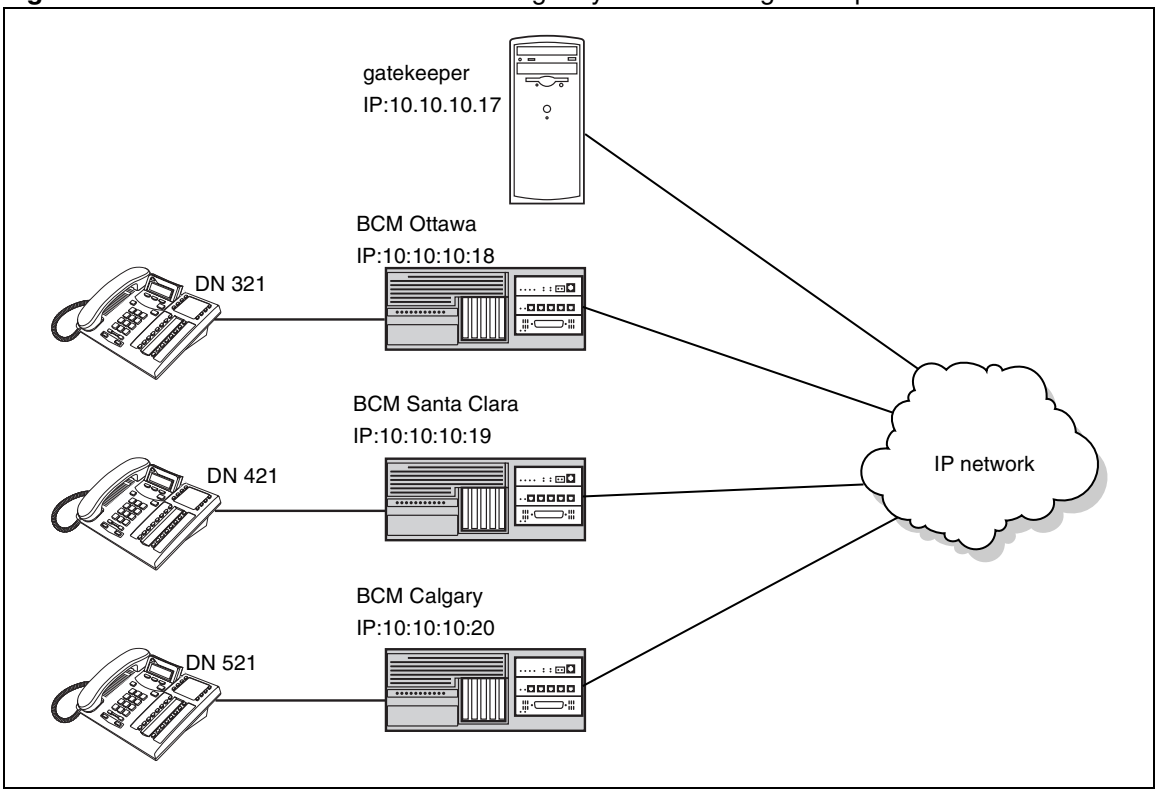
If selecting **GateKeeperRouted** or **GateKeeperResolved**, in the **Gatekeeper IP** box type the IP address of the machine that is running the gatekeeper.

If selecting **GateKeeperRouted** or **GateKeeperResolved**, in the **Alias Names** box type one or more alias names for the gateway. For information on setting alias names, see "Alias names" on page 80.

Gatekeeper call scenarios

This section explains what must be set up, and how a call would be processed for the two types of gatekeeper configurations. Figure 42 on page 82 shows a network with three Business Communications Managers and a gatekeeper.

Figure 42 Business Communications Manager systems with a gatekeeper



This example explains how a call from DN 321 in Ottawa would be made to DN 421 in Santa Clara. It assumes that call signalling is set to Gatekeeper Resolved and no pre-granted ARQ has been issued:

1. Business Communications Manager Ottawa sends an AdmissionRequest (ARQ) to the gatekeeper for DN 421.
2. The gatekeeper resolves DN 421 to 10.10.10.19 and returns this IP in an AdmissionConfirm to the Business Communications Manager Ottawa.
3. Business Communications Manager Ottawa sends the call Setup message for DN 421 to the gateway at 10.10.10.19, and the call is established.

If call signalling is set to Gatekeeper Routed and no pre-granted ARQ has been issued:

1. Business Communications Manager Ottawa send an AdmissionRequest to the gatekeeper for DN 421.
2. The gatekeeper resolves DN 421 to 10.10.10.17.
3. Business Communications Manager Ottawa sends the call Setup message for DN421 to the gatekeeper (10.10.10.17), which forwards it to the gateway at 10.10.10.19, and the call is established.

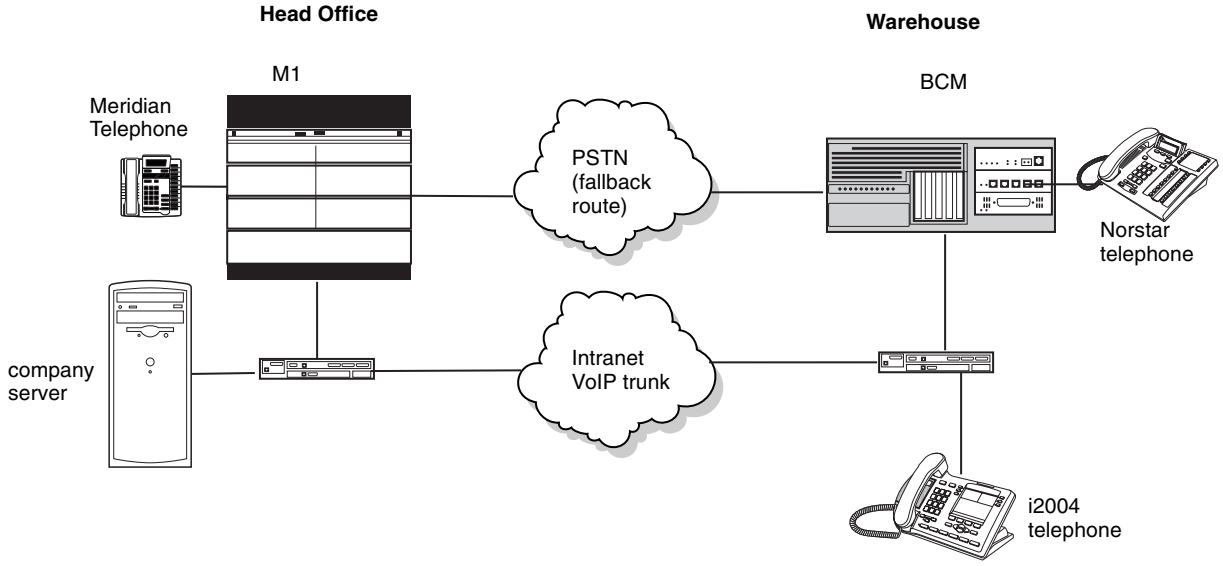
Chapter 5
Typical applications

This section explains several common installation scenarios and provides examples for how to use VoIP trunks and IP telephony to enhance your network.

M1 to Business Communications Manager over IP trunks

The Business Communications Manager 2.5 can connect with a Meridian 1 to extend an existing network. In this type of installation, capabilities of the M1 are available to phones on the Business Communications Manager 2.5. For example, a company that has a M1 in a Head Office may want to set up a warehouse in another region. The warehouse can then call the head office across VoIP lines, bypassing long-distance tolls.

Figure 43 M1 to Business Communications Manager network diagram



To set up this system:

1. Make sure the M1 ITG meets the following requirements:
   - ITG Kit [NTZC44BA] Delta 24.24
   - Rls25.30
   - S/W Packages 57, 58, 59, 145, 147, 148, 160
2. Set up the M1 ESN programming (CDP/UDP). For information on this, see your M1 documentation.
3. On the Business Communications Manager 2.5 Unified Manager:
   - Set up outgoing call configuration for the VoIP gateway.
   - Set up a remote gateway for the Meridian 1.

- Set phones to receive incoming calls through target lines.
- Configure the PSTN fallback and enable QoS on both systems.
- Activate and program CDP or UDP. For information on CDP and UDP, see the *Business Communications Manager 2.5 Programming Operations Guide*.

MCDN functionality

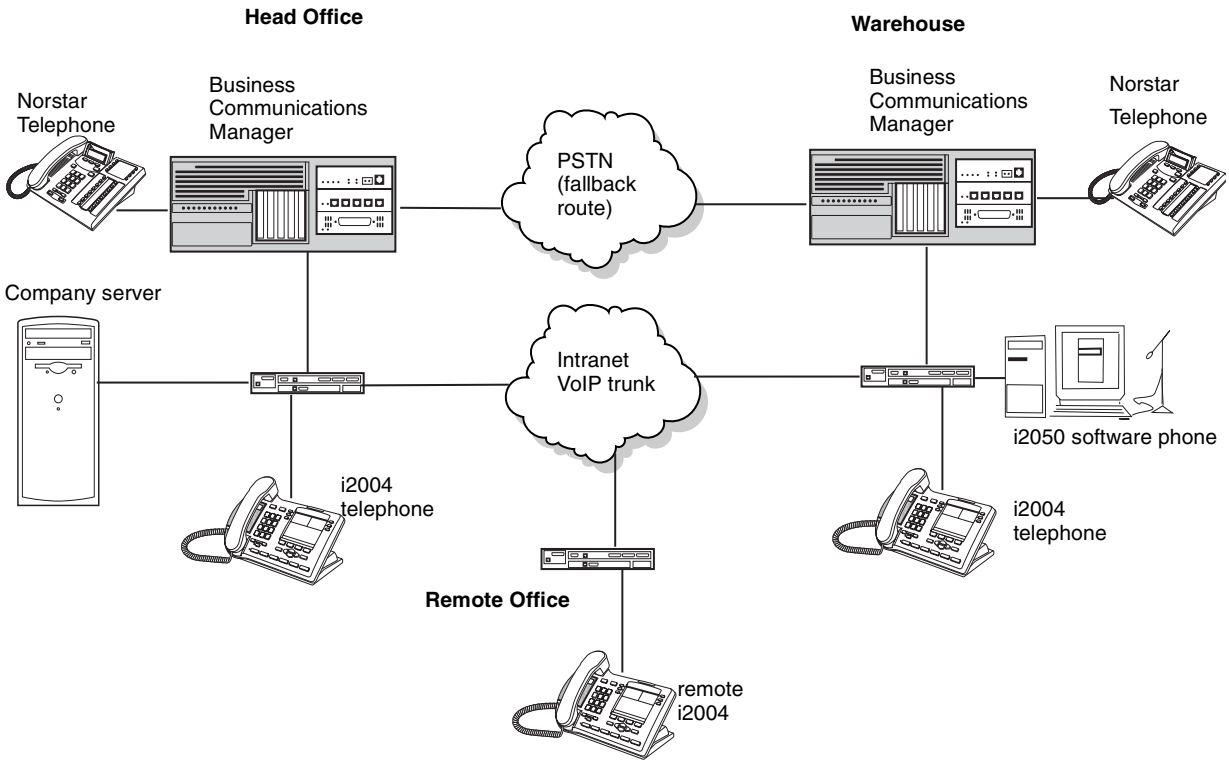
To use MCDN functionality over PRI, set up:

- MCDN PRI settings on the M1. For information on this, see your M1 documentation.
- SL-1 (MCDN) keycodes on the Business Communications Manager 2.5.

Multiple Business Communications Manager systems across VoIP trunks

This system allows multiple offices to connect across the company Intranet. This installation allows for CallPilot to direct calls throughout the system. Full toll bypass occurs through the tandem setup, meaning that any user can call any DN without long distance charges. Users have full access to system users, applications, PSTN connections, Unified Messaging. The network diagram shows two Business Communications Managers, but additional base units can be added.

Figure 44 Multiple Business Communications Manager systems network diagram



To set up this system:

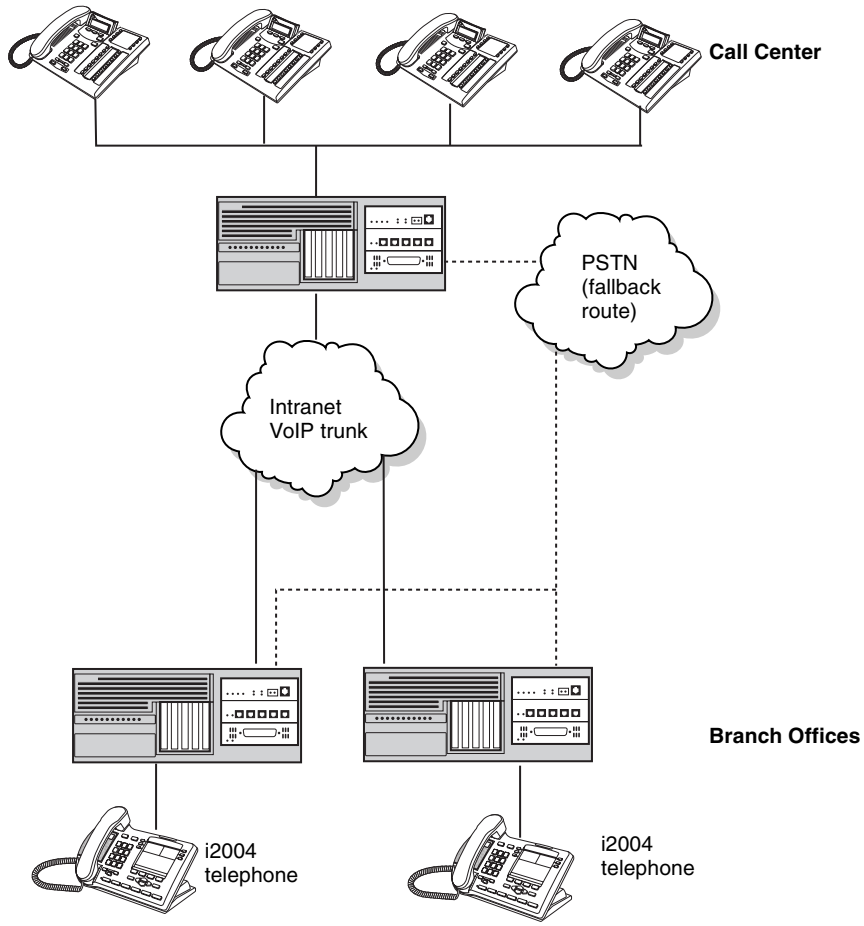
1. Ensure that the existing network can support the additional VoIP traffic.
2. Coordinate a dialing plan.
3. On each Business Communications Manager 2.5 system:
   - Set up outgoing call configuration for the VoIP gateway.
   - Set up a remote gateway for other Business Communications Managers or NetMeeting users.
   - Set phones to receive incoming calls through target lines.
   - Configure the PSTN fallback and enable QoS on both systems.
4. Reboot each system.

This system uses fallback to PSTN so that if traffic between the Business Communications Manager systems becomes too heavy, calls are routed across the PSTN.

Multi-location chain with call center

In this installation, one Business Communications Manager runs a Call Center and passes calls to the appropriate branch offices, each of which have a Business Communications Manager. A typical use of this would be a 1-800 number that users world-wide can call, who are then directed the the remote office best able to handle their needs.

Figure 45 M1 to Business Communications Manager network diagram



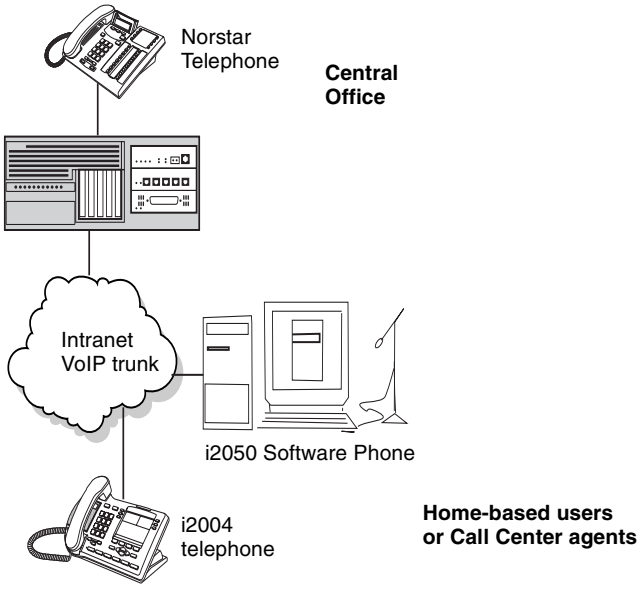
To set up this system:

1. Ensure that the existing network can support the additional VoIP traffic.
2. Coordinate a dialing plan.
3. On each Business Communications Manager 2.5 system:
   - Set up outgoing call configuration for the VoIP gateway.
   - Set up a remote gateway for other Business Communications Managers.
   - Set phones to receive incoming calls through target lines.
   - Configure the PSTN fallback and enable QoS on both systems.
4. Reboot each system.
5. Set up a Call Center on the central Business Communications Manager.

Business Communications Manager to IP Telephones

This system allows for home-based users or Call Center agents to use the full capabilities of the Business Communications Manager, including system users, applications and PSTN connections. This system does not require VoIP trunk configuration. This system functions in a similar mannger to the system described in "Multi-location chain with call center" on page 87. This system is less expensive and on a smaller scale. However, it does not offer PSTN fallback.

Figure 46 M1 to Business Communications Manager network diagram



To set up this system:

1. Ensure that each remote user has a network connection capable of support VoIP traffic, such as DSL or cable.
2. On the Business Communications Manager, set up the system to support IP telephones.
3. At the remote user's location, install and configure i20XX telephone.
4. Register each phone and provide it with a DN.

Appendix A
Networking

This appendix provides information on making your network run more efficiently.

Determining the bandwidth requirements

The design process starts with the an IP telephony bandwidth forecast. The bandwidth forecast determines the following:

- LAN requirements: LAN must have enough capacity for the number of calls plus the overhead
- WAN requirements: WAN must have enough capacity for the number of calls plus the overhead

Determining WAN link resources

For most installations, IP telephony traffic travels over WAN links within the intranet. WAN links are the highest recurring expenses in the network and they are often the source of capacity problems in the network. WAN links require time to receive financial approval, provision and upgrade, especially inter-LATA (Local Access and Transport Area) and international links. For these reasons, it is important to determine the stateof WAN links in the intranet before installing the IP telephony.

Link utilization

This procedure explains how to determine and adjust link utilization:

1. Get a current topology map and link utilization report of the intranet. A visual inspection of the topology can indicate the WAN links anticipated to deliver IP telephony traffic.
2. Record the current utilization of the links that will be handling IP telephony traffic. For example, the link utilization can be an average of a week, a day, or one hour. To be consistent with the considerations, get the peak utilization of the trunk.
3. Determine the available spare capacity. Business Communications Manager intranets are subject to capacity planning controls that ensure that capacity use remains below a determined utilization level. For example, a planning control can state that the utilization of a 56 kbit/s link during the peak hour must not exceed 50%. For example, for a T1 link, the threshold is higher, for example at 85%. The carrying capacity of the 56 kbit/s link can be 28 kbit/s, and for the T1, 1.3056 Mbit/s. In some organizations the thresholds can be lower than those used in this example. In the event of link failures, spare capacity for rerouting traffic is required.

Some WAN links can exist on top of layer 2 services such as Frame Relay and Asychronous Transfer Mode (ATM). The router-to-router link is a virtual circuit, which is subject not only to a physical capacity, but also to a logical capacity limit. The installer or administrator needs to obtain the physical link capacity and the QoS parameters. The important QoS parameters are CIR (committed information rate) for Frame Relay, and MCR (maximum cell rate) for Asynchronous Transfer Mode (ATM).

The difference between the current capacity and its acceptable limit is the available capacity. For example, a T1 link used at 48% during the peak hour with a planning limit of 85% has an available capacity of approximately 568 kbit/s.

Network Engineering

Engineer the network for worst-case numbers to indicate the spare bandwidth a LAN must have to handle peak traffic. It is important to plan that the LAN/WAN can handle the IP telephony traffic using the defined codec, without delay or packet loss. The installer or administrator must select one configuration and then set up the LAN/WAN so there is more bandwidth than the IP telephony output.

Table 10 on page 93 provides bandwidth characteristics for the transmission of voice over IP for various link types given codec type and payload sizes. The bandwidths provided in Table 10 on page 93 explain the continuous transmission of a unidirectional media stream.

The peak bandwidth and average bandwidth requirements for a normal two-way call must take into account the affects of full and half duplex links and the affects of silence suppression. See Table 11 on page 94 and Table 12 on page 95 for voice Gateway bandwidth requirements.

Peak bandwidth is the amount of bandwidth that the link must provide for each call. Considering voice traffic only, the number of calls a link can support is:

$$\text{Number of calls} = \left(\frac{\text{Usable Link bandwidth}}{\text{peak bandwidth per call}}\right)$$

Number of Calls = Usable Link Bandwidth / peak Bandwidth per call

The average bandwidth takes into account the affects of silence suppression, which over time tends to reduce bandwidth requirements to 50% of the continuous transmission rate. The affects of silence suppression on peak bandwidth requirements differ depending on whether the link is half-duplex or full-duplex. See Appendix B, “Silence compression,” on page 103 for more information.

When engineering total bandwidth requirements for LANs and WANs, additional bandwidth must be allocated for data. Refer to standard Ethernet engineering tables for passive 10BaseT repeater hubs. Refer to the manufacturer’s specification for intelligent 10BaseT layer switches. WAN links must take into account parameters such as normal link utilization and committed information rates.

Table 10 Voice over IP Transmission Characteristics for unidirectional continuous media stream

Codec Type	Payload Size		IP Packet	Ethernet B/W[2]	PPP B/W	FR B/W
	ms	Bytes	Bytes	kbit/s	kbit/s	kbit/s
G.711 (64 kb/s)	10	80	120	116.8	97.6	103.2
	20	160	200	90.4	80.8	83.6
	30	240	280	81.6	75.2	77.1
G.729 (8 kb/s)	10	10	50	60.8	41.6	47.2
	20	20	60	34.4	24.8	27.6
	30	30	70	25.6	19.2	21.1
G.723.1 (6.3 kb/s)	30	24	64	24.0	17.6	19.5
G.723.1 (5.3 kb/s)	30	20	60	22.9	16.5	18.4

Notes:

1) Gray Background indicated payload sizes used by Business Communications Manager 2.5 for transmission. Other values listed indicate payload sizes that the Business Communications Manager 2.5 can receive.

2) Ethernet bandwidth includes the 14 byte Ethernet frame overhead plus a 12 byte inter-frame gap.

Bandwidth Requirements on Half Duplex Links

Table 11 on page 94 provides bandwidth requirements for normal two-way voice calls on a half-duplex link for a variety of link protocols, codec types and payload sizes.

With no silence suppression, both the transmit path and the receive path continuously transmit voice packets. Therefore, the peak bandwidth requirement per call on half-duplex links is:

$$\text{Peak Bandwidth per call} = 2(\text{Continuous Transmission Rate})$$

(Half Duplex links, No Silence Suppression)

On half-duplex links with silence suppression enabled, the half-duplex nature of normal voice calls allows the sender and receiver to share the same bandwidth on the common channel; while the sender is talking, the receiver is quiet. Since only one party is transmitting at a time, silence suppression reduces the peak bandwidth requirement per call on a half-duplex link to::

$$\text{Peak Bandwidth per call} = 1(\text{Continuous Transmission Rate})$$

peak Band Width per call = 1 * Continuous Transmission Rate

(Half Duplex links, With Silence Suppression)

Table 11 Bandwidth Requirements per BCM Gateway port for half-duplex links.

Codec Type	Payload Size	Ethernet B/W[2]			PPP B/W			FR B/W		
		No SP	Silence Suppression		No SP	Silence Suppression		No SP	Silence Suppression	
		peak	peak	Avg	peak	peak	Avg	peak	peak	Avg
	ms	kbit/s	kbit/s	kbit/s	kbit/s	kbit/s	kbit/s	kbit/s	kbit/s	kbit/s
G.711 (64 kb/s)	10	233.6	233.6[3]	233.6[3]	195.2	195.2[3]	195.2[3]	206.4	206.4[3]	206.4[3]
	20	180.8	180.8[3]	180.8[3]	161.6	161.6[3]	161.6[3]	167.2	167.2[3]	167.2[3]
	30	163.2	163.2[3]	163.2[3]	150.4	150.4[3]	150.4[3]	154.2	154.2[3]	154.2[3]
G.729 (8 kb/s)	10	121.6	60.8	60.8	83.2	41.6	41.6	94.4	47.2	47.2
	20	68.8	34.4	34.4	49.6	24.8	24.8	55.2	27.6	27.6
	30	51.2	25.6	25.6	38.4	19.2	19.2	42.2	21.1	21.1
G.723.1 (6.3 kb/s)	30	48.0	24.0	24.0	35.2	17.6	17.6	39.0	19.5	19.5
G.723.1 (5.3 kb/s)	30	45.8	22.9	22.9	33.0	16.5	16.5	36.8	18.4	18.4

Notes:

1) Gray background indicates payload sizes used by Business Communications Manager 2.5 for transmission. Other values listed indicate payload sizes that BCM can receive.

2) Ethernet bandwidth includes the 14 byte Ethernet frame overhead plus a 12 byte inter-frame gap.

3) G.711 does not support silence suppression.

Bandwidth Requirements on Full Duplex Links

Table 12 on page 95 provides bandwidth requirements for normal two-way voice calls on a full-duplex link for a variety of link protocols, codec types and payload sizes. Bandwidths for full-duplex links are stated in terms of the individual transmit and receive channels. For instance a 64 kbits full duplex link (e.g. a DS0 on T1 link) has 64 kbits in the transmit direction and 64 kbits in the receive direction.

With no silence suppression, both the transmit path and the receive path continuously transmit voice packets. Enabling silence suppression on full-duplex links reduces the average bandwidth. However, since transmit and receive paths use separate channels, the peak bandwidth per call per channel does not change. Therefore, peak bandwidth requirements per channel (Rx or Tx) per call on a full-duplex link is::

$$\text{Peak Bandwidth per channel per call} = 2(\text{Continuous Transmission Rate})$$

(Full Duplex links, With or Without Silence Suppression)

The bandwidth made available by silence suppression on full-duplex links with continuous transmission rate – average bandwidth requirement, is available for lower priority data applications that can tolerate increased delay and jitter.

Table 12 Bandwidth Requirements per BCM Gateway port for Full-duplex links.

Codec Type	**Payload Size**	**Ethernet B/W[2]**			**PPP B/W**			**FR B/W**		
		No SP	Silence Suppression		**No SP**	Silence Suppression		**No SP**	Silence Suppression	
		peak	peak	Avg	peak	peak	Avg	peak	peak	Avg
	msec	kbit/s	kbit/s	kbit/s	kbit/s	kbit/s	kbit/s	kbit/s	kbit/s	kbit/s
G.711 (64 kb/s)	10	116.8	116.8	116.8[3]	97.6	97.6	97.6[3]	103.2	103.2	103.2[3]
	20	90.48	90.4	90.4[3]	80.8	80.8	80.8[3]	83.6	83.6	83.6[3]
	30	81.6	81.6	81.6[3]	75.2	75.2	75.2[3]	77.1	77.1	77.1[3]
G.729 (8 kb/s)	10	60.8	60.8	30.4	41.6	41.6	20.8	47.2	47.2	23.6
	20	34.2	34.4	17.2	24.8	24.8	12.4	27.6	27.6	13.8
	30	25.6	25.6	12.8	19.2	19.2	9.6	21.1	21.1	10.6
G.723.1 (6.3 kb/s)	30	24.0	24.0	12.0	17.6	17.6	8.8	19.5	19.5	9.8
G.723.1 (5.3 kb/s)	30	22.9	22.9	11.5	16.5	16.5	8.3	18.4	18.4	9.2

Notes:

1) Gray background indicates payload sizes used by Business Communications Manager 2.5 for transmission. Other values listed indicate payload sizes that Business Communications Manager can receive.

2) Ethernet bandwidth includes the 14 byte Ethernet frame overhead plus a 12 byte inter-frame gap.

3) G.711 does not support silence suppression. Therefore the average bandwidth is the same as the peak bandwidth.

4) Bandwidths stated per channel (Rx or Tx).

LAN Engineering Examples

Example 1: LAN engineering - voice calls

Consider a site with four Business Communications Manager IP telephony ports. Assume a preferred codec of G.729, which uses a voice payload of 20 ms. Silence compression is enabled. The Ethernet LAN is half-duplex. Ethernet LAN may also be full duplex.

Given the above, what is the peak traffic in kbit/s that IP telephony will put on the LAN?

From Table 11 on page 94, the peak transmission bandwidth for G.729 with silence suppression enabled on a half-duplex link is 34.4 kbit/s per call or 137.6 kbit/s for all four calls.

WAN engineering

Wide Area Network (WAN) links are typically full-duplex links - both talk and listen traffic use separate channels. For example, a T1 link uses a number of 64 kbit/s (DS0) duplex channels allowing *64 kbit/s for transmit path and n*64 kbit/s for the receive path.

(WAN links may also be half-duplex.)

Example 1: WAN engineering - voice calls

Consider a site with four IP telephony ports and a full-duplexWAN link using PPP. The preferred codec is G.729 kbit/s, which uses a voice payload of 20 ms. Silence compression is enabled.

Given the above, what is the peak traffic in kbit/s that IP telephony will put on theWAN?

From Table 12 on page 95, the peak transmission rate for G.729 is 24.8 kbit/s per call or 99.2 kbit/s in each direction for all 4 calls. In other words, in order to support four G.729 calls, the WAN link must have at least 99.2 kbit/s of usable bandwidth (in each direction).

From Table 12 on page 95, the average bandwidth for each call is 12.4 kbit/sec per channel or 49.4 kbit/s for all 4 calls for each channel. Low priority data applications can make use of bandwidth made available by silence suppression.

Additional feature configuration

This section contains additional information on configuring your network to run efficiently.

Setting Non-linear processing

Non-linear processing should normally be enabled.

To set non-linear processing:

1. In Unified Manager, open **Services, IP Telephony**, and click on **H.323 settings**. The H.323 parameters appear in the right window.
2. Click the **Non-linear processing** drop-down menu, and select either **Enabled** or **Disabled**.

Determining network loading caused by IP telephony traffic

At this point, the installer or administrator has enough information to load the IP telephony traffic on the intranet.

Consider the intranet has the topology as shown Figure 47 on page 97, and the installer or administrator wants to know in advance the amount of traffic on a specific link, R4-R5. Consider there are four IP telephony ports per site.

Each site supports four VoIP ports. Assume the codex is G.729 Annex B, 20 ms payload. Assuming full-duplex links, peak bandwidths per call are from Table 12 on page 95 which is between 24.8 kbit/s and 27.6 kbit/s peak transmission or approximately 28 kbit/s.

Route R1-R2 needs to support 4 VoIP Calls. R4-R5 needs to support eight VoIP calls. The incremental peak bandwidth for VoIP traffic is therefore:

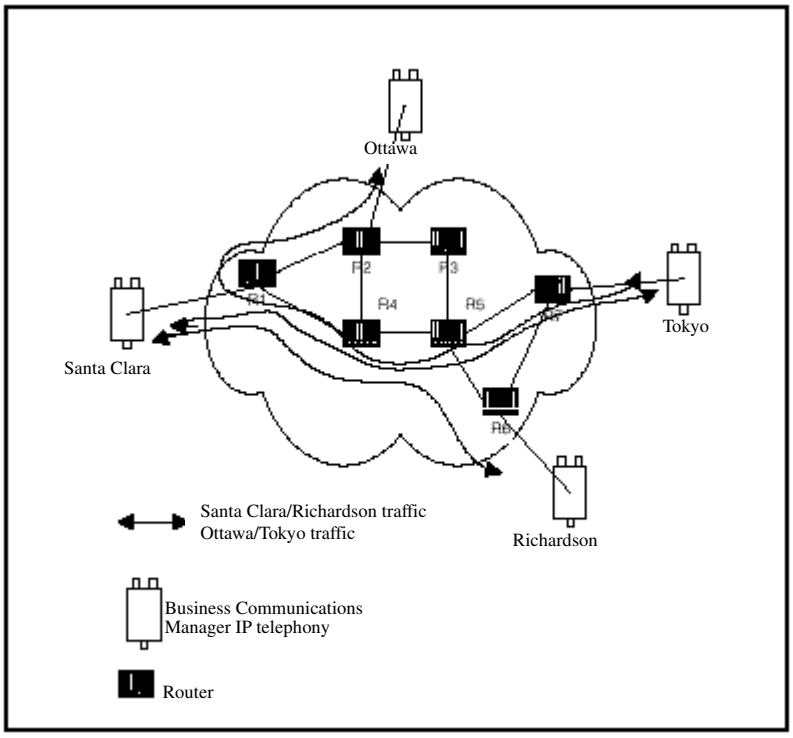
$$\text{R1-R2 peak VoIP Load} = 4(28\ \text{kbit/s}) = 112\text{kbit/s}$$

$$\text{R4-R5 peak VoIP Load} = 8(28\ \text{kbit/s}) = 112\text{kbit/s}$$

With BCM VoIP gateway bandwidth requirements and `Traceroute` measurements, the R4-R5 link is expected to support the Santa Clara/Richardson, Santa Clara/Tokyo and the Ottawa/Tokyo traffic flows. The other IP telephony traffic flows do not route over R4-R5. A peak of eight calls can be made over R4-R5 for the four IP telephony ports per site. R4-R5 needs to support the incremental bandwidth of 8 x 12 = 96 kbit/s.

To complete this exercise, the traffic flow from every site pair needs to be summed to calculate the load on each route and loaded to the link.

Figure 47 Calculating network load with IP telephony traffic



Enough link capacity

Table 13 on page 98 sorts the computations so that for each link, the available link capacity is compared against the additional IP telephony load. For example, on link R4-R5, there is capacity (568 kbit/s) to allow for the additional 96 kbit/s of IP telephony traffic.

Table 13 Link capacity example

Link		Utilization (%)		Available capacity kbit/s	Incremental IP telephony load		Enough capacity?
End Points	Capacity kbit/s	Threshold	Used		Site pair	Traffic kbit/s	
R1-R2	1536	85	75	154	Santa Clara/ Ottawa Santa Clara/ Tokyo	15.5	Yes
R1-R3	1536						
R2-R3	1536						
R2-R4	1536						
R4-R5	1536	85	48	568	Santa Clara/ Richardson Ottawa/Tokyo Santa Clara/ Tokyo	24	Yes

Some network management systems have network planning modules that determine network flows. These modules provide more detailed and accurate analysis as they can include correct node, link and routing information. They also help to determine network strength by conducting link and node failure analysis. By simulating failures, re-loading network and re-computed routes, the modules indicate where the network can be out of capacity during failures.

Not enough link capacity

If there is not enough link capacity, consider one or more of the following options:

- Use the G.723.1 codec. Compared to the default G.729 codec with 20 ms payload, the G.723.1 codecs use 29% to 33% less bandwidth.
- Upgrade the bandwidth for the links.

Other intranet resource considerations

Bottlenecks caused by non-WAN resources do not occur often. For a more complete evaluation consider the impact of incremental IP telephony traffic on routers and LAN resources in the intranet. The IP telephony traffic moves across LAN segments that are saturated, or routers whose central processing unit (CPU) utilization is high.

Implementing the network

LAN engineering

To minimize the number of router hops between the systems, connect the gateways to the intranet. Ensure that there is enough bandwidth on the WAN links shorter routes. Place the gateway and the LAN router near the WAN backbone. This prevents division of the constant bit-rate IP telephony traffic from bursty LAN traffic, and makes easier the end-to-end Quality of Service engineering for packet delay, jitter and packet loss.

Getting the best results from your system

Further network analysis

This section describes how to examine the sources of delay and error in the intranet. This section discusses several methods for reducing one-way delay and packet loss. The key methods are:

- "Reduce link delay" on page 100
- "Reducing hop count" on page 100
- "Adjust the jitter buffer size" on page 101

Components of delay

End-to-end delay is the result of many delay components. The major components of delay are as follows:

- Propagation delay: Propagation delay is the result of the distance and the medium of links moved across. Within a country, the one-way propagation delay over terrestrial lines is under 18 ms. Within the U.S., the propagation delay from coast-to-coast is under 40 ms. To estimate the propagation delay of long-haul and trans-oceanic circuits, use the rule of thumb of 1 ms per 100 terrestrial miles.
  If a circuit goes through a satellite system, estimate each hop between earth stations adds 260 ms to the propagation delay.

- Serialization delay: The serialization delay is the time it takes to transmit the voice packet one bit at a time over a WAN link. The serialization delay depends on the voice packet size and the link bandwidth, and is the result of the following formula:

$$\text{serialization delay in ms} = 8\left(\frac{\text{IP packet size in bytes}}{\text{link bandwidth in kbit/s}}\right)$$

- Queuing delay: The queuing delay is the time it takes for a packet to wait in the transmission queue of the link before it is serialized. On a link where packets are processed in a first come first served order, the average queuing time is in milliseconds and is the result of the following formula:

$$\text{queuing time in ms} = 8\left(\frac{\text{average IP packet size in bytes}}{(1-p)(\text{link bandwidth in kbit/s})}\right)$$

  The average size of intranet packets carried over WAN links generally is between 250 and 500 bytes. Queueing delays can be important for links with bandwidth under 512 kbit/s, while with higher speed links they can allow higher utilization levels.
- Routing and hop count: Each site pair takes different routes over the intranet. The route taken determines the number and type of delay components that add to end-to-end delay. Sound routing in the network depends on correct network design.

Reduce link delay

In this and the next few sections, the guidelines examine different ways of reducing one-way delay and packet loss in the network.

The time taken for a voice packet to queue on the transmission buffer of a link until it is received at the next hop router is the link delay. Methods to reduce link delays are:

- Upgrade link capacity to reduce the serialization delay of the packet. This also reduces the utilization of the link, reducing the queueing delay. Before upgrading a link, check both routers connected to the link for the upgrade and ensure correct router configuration guidelines.
- Change the link from satellite to terrestrial to reduce the link delay by approximately 100 to 300 ms.
- Put into operation a priority queueing rule.
- Identify the links with the highest use and the slowest traffic. Estimate the link delay of these links using Traceroute. Contact your service provider for help with improving your QoS.

Reducing hop count

To reduce end-to-end delay reduce hop count, especially on hops that move across WAN links. Some of the ways to reduce hop count include:

- Improve meshing. Add links to help improve routing, adding a link from router1 to router4 instead of having the call routed from router 1 to router 2 to router 3 to router 4 reducing the hop count by two.
- Router reduction. Join co-located gateways on one larger and more powerful router.

Adjust the jitter buffer size

The parameters for the voice jitter buffer directly affect the end-to-end delay and audio quality. IP telephony dynamically adjusts the size of the jitter buffer to adjust for jitter in the network. The network administrator sets the starting point for the jitter buffer.

Lower the jitter buffer to decrease one-way delay and provide less waiting time for late packets. Late packets that are lost are replaced with silence. Quality decreases with lost packets. Increase the size of the jitter buffer to improve quality when jitter is high.

IP telephony fax calls use a fixed jitter buffer that does not change the hold time over the duration of the call. Fax calls are more prone to packet loss. In conditions of high jitter, increase delay through the use of a deeper jitter buffer. To allow for this increase, IP telephony provides a separate jitter buffer setting for fax calls.

Reduce packet errors

Packet errors in intranets correlate to congestion in the network. Packet errors are high because the packets are dropped if they arrive faster than the link can transmit. Identify which links are the most used to upgrade. This removes a source of packet errors on a distinct flow. A reduction in hop count provides for less occurrences for routers and links to drop packets.

Other causes of packet errors not related to delay are as follows:

- reduced link quality
- overloaded CPU
- saturation
- LAN saturation
- limited size of jitter buffer

If the underlying circuit has transmission problems, high line error rates, outages, or other problems, the link quality is reduced. Other services such as X.25 or frame relay can affect the link. Check with your service provider for information.

Find out what the router threshold CPU utilization level is, and check if the router conforms to the threshold. If a router is overloaded, the router is continuously processing intensive tasks. Processing intensive tasks prevents the router from forwarding packets. To correct this, reconfigure or upgrade the router.

Routers can be overloaded when there are too many high-capacity and high-traffic links configured on it. Ensure that routers are configured to vendor guidelines.

Saturation refers toa situation where too many packets are on the intranet. Packets can be dropped on improperly planned or damaged LAN segments.

Packets that arrive at the destination late are not placed in the jitter buffer and are lost packets. See "Adjust the jitter buffer size" on page 101.

Routing issues

Routing problems cause unnecessary delay. Some routes are better than other routes. The Traceroute program allows the user to detect routing anomalies and to correct these problems.

Possible high-delay differences causes are:

- routing instability
- wrong load splitting
- frequent changes to the intranet
- asymmetrical routing

Post-installation network measurements

The network design process is continuous, even after implementation of the IP telephony and commissioning of voice services over the network. Network changes in regard to real IP telephony traffic, general intranet traffic patterns, network controls, network topology, user needs and networking technology can make a design invalid or non-compliant with QoS objectives. Review designs against prevailing and trended network conditions and traffic patterns every two to three weeks at the start, and after, four times a year. Ensure that you keep accurate records of settings and any network changes on an ongoing basis.

Ensure that you have valid processes to monitor, analyze, and perform design changes to the IP telephony and the corporate intranet. These processes ensure that both networks continue to conform to internal quality of service standards and that QoS objectives are always met.

Appendix B
Silence compression

Silence compression reduces bandwidth requirements by as much as 50%. This appendix explains how silence compression functions. For information on enabling silence compression in VoIP gateways, see "Setting Silence Compression" on page 54.

G.723.1 and G.729, Annex B support Silence compression.

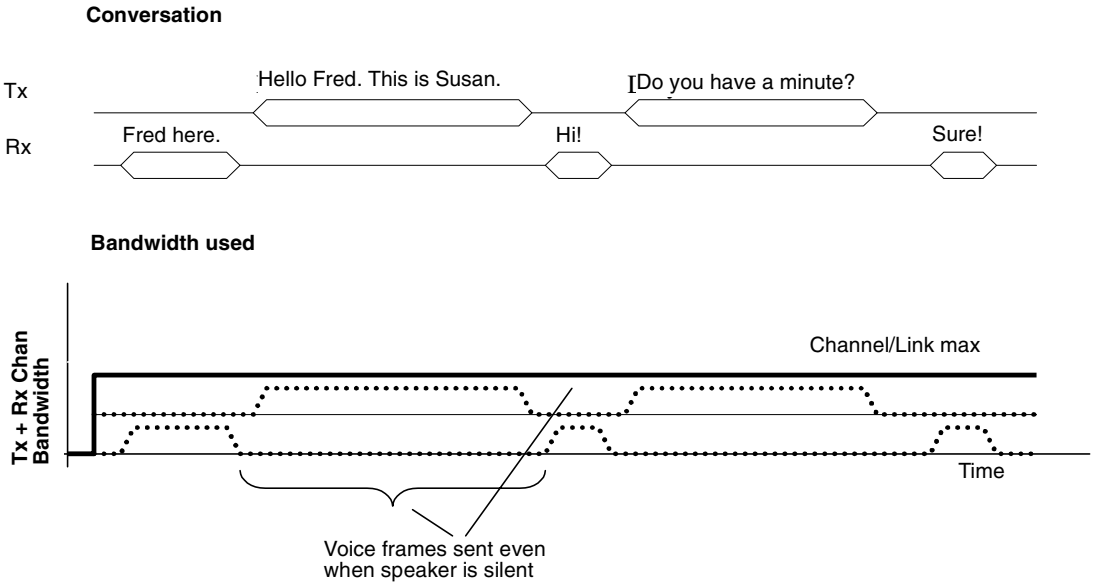
A key to VoIP Gateways in business applications is reducing WAN bandwidth use. Beyond speech compression, the best bandwidth-reducing technology is silence compression, also known as silence compression or Voice Activity Detection (VAD). Silence compression technology identifies the periods of silence in a conversation, and stops sending IP speech packets during those periods. Telco studies show that in a typical telephone conversation, only about 36-40% of a full-duplex conversation is active. When one person talks, the other listens. This is half-duplex. And there are important periods of silence during speaker pauses between words and phrases. By applying silence compression, average bandwidth use is reduced by the same amount. This 50%-reduction in average bandwidth requirements develops over a 20-to-30-second period as the conversation switches from one direction to another.

When a voice is being transmitted, it uses the full rate or continuous transmission rate. The affects of silence compression on peak bandwidth requirements differ depending on whether the link is half-duplex or full duplex.

Silence compression on Half Duplex Links

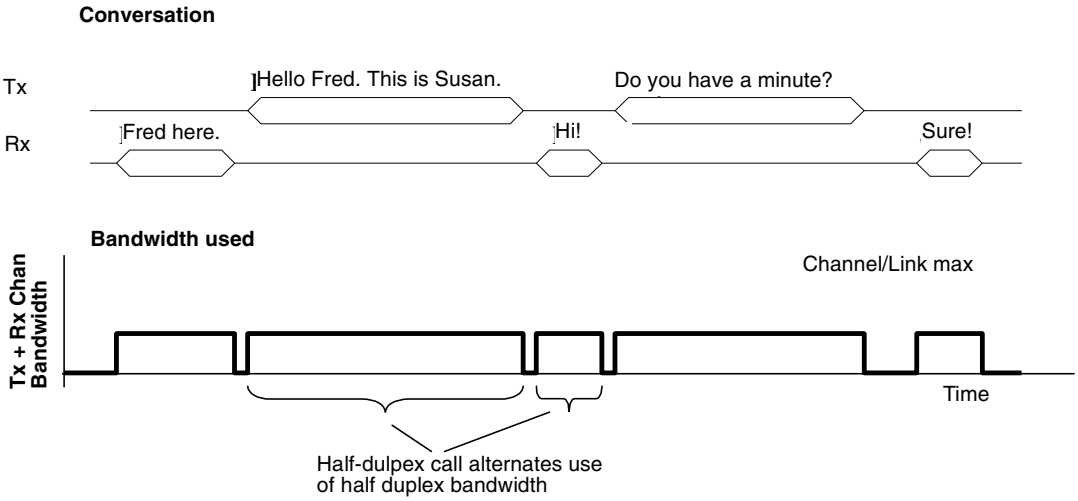
Figure 48 on page 104 shows the bandwidth requirement for one call on a half duplex link without silence compression. Since the sender and receiver share the same channel, the peak bandwidth is double the full transmission rate. Because voice packets are transmitted even when a speaker is silent, the average bandwidth used is equal to the full transmission rate.

Figure 48 One Call on a Half Duplex Link Without Silence compression



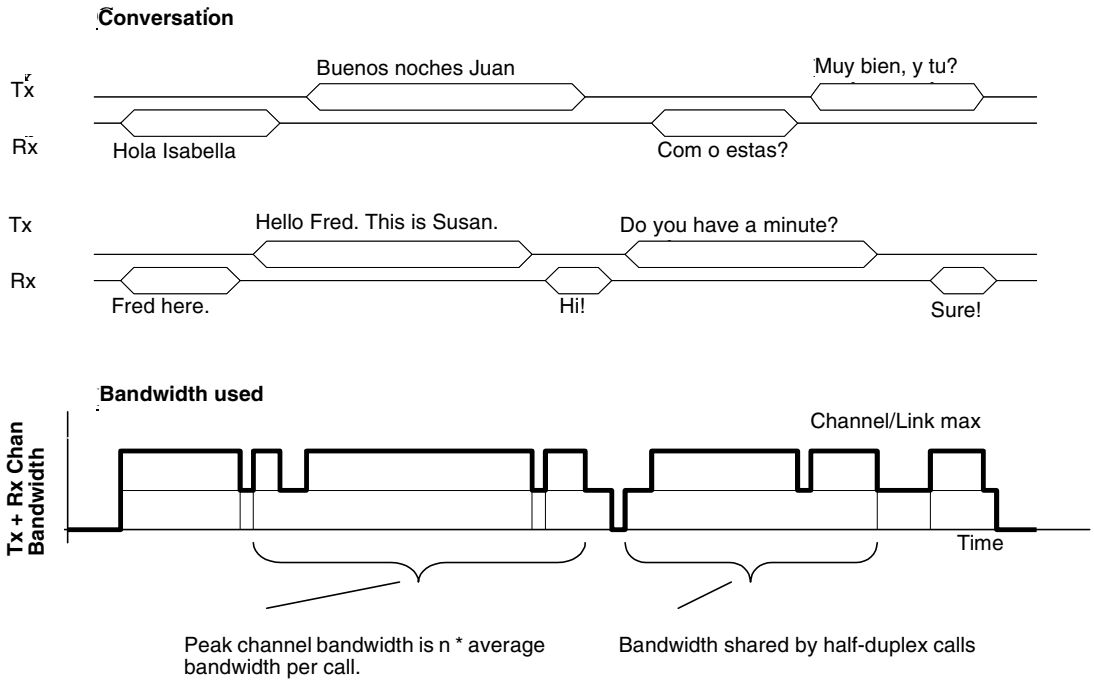
When silence compression is enabled, voice packets are only sent when a speaker is talking. In a typical voice conversation while one speaker is talking, the other speaker is listening – a half duplex conversation. Figure 49 on page 104 shows the peak bandwidth requirements for one call a half-duplex link with silence compression enabled. Because the sender and receiver alternate the use of the shared channel, the peak bandwidth requirement is equal to the full transmission rate. Only one media path is present on the channel at one time.

Figure 49 One Call on a Half Duplex Link With Silence compression



The affect of silence compression on half-duplex links is therefore to reduce the peak and average bandwidth requirements by approximately 50% of the full transmission rate. Because the sender and receiver are sharing the same bandwidth, this affect can be aggregated for a number of calls. Figure 50 on page 105 below shows the peak bandwidth requirements for two calls on a half-duplex link with silence compression enabled. The peak bandwidth for all calls is equal to the sum of the peak bandwidth for each individual call. In this case, that is twice the full transmission rate for the two calls.

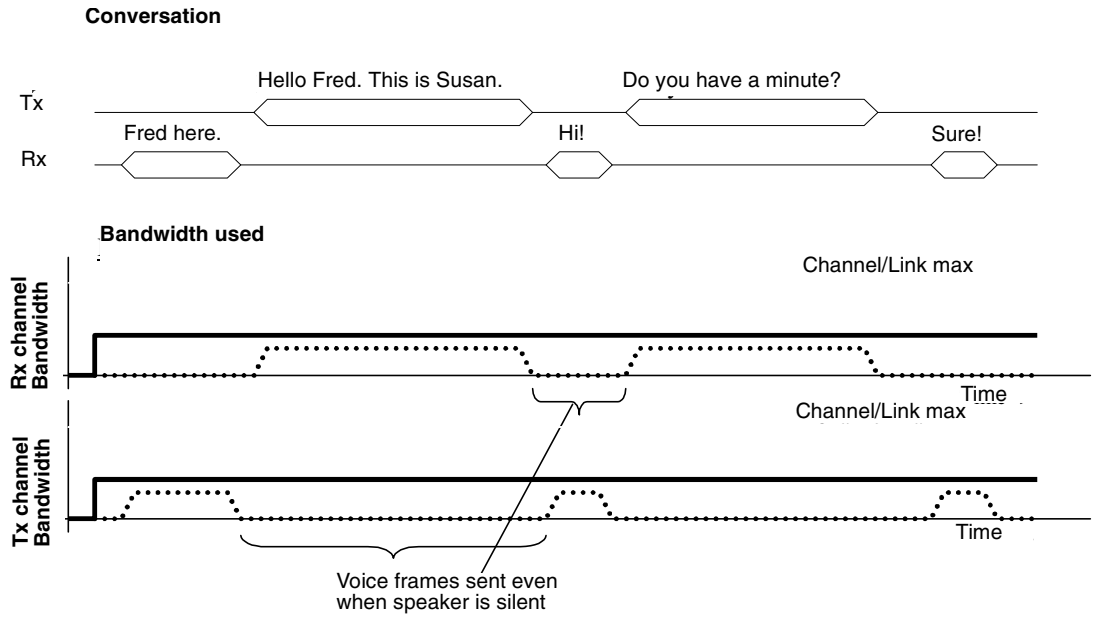
Figure 50 Two Calls on a Half Duplex Link With Silence compression



Silence compression on Full Duplex Links

On full duplex links, the transmit path and the receive path are separate channels with bandwidths usually quoted in terms of individual channels. Figure 51 on page 106 shows the peak bandwidth requirements for one call on a full duplex link without silence compression. Because voice packets are transmitted, even when a speaker is silent, the peak bandwidth and the average bandwidth used is equal to the full transmission rate for both the transmit and the receive channel.

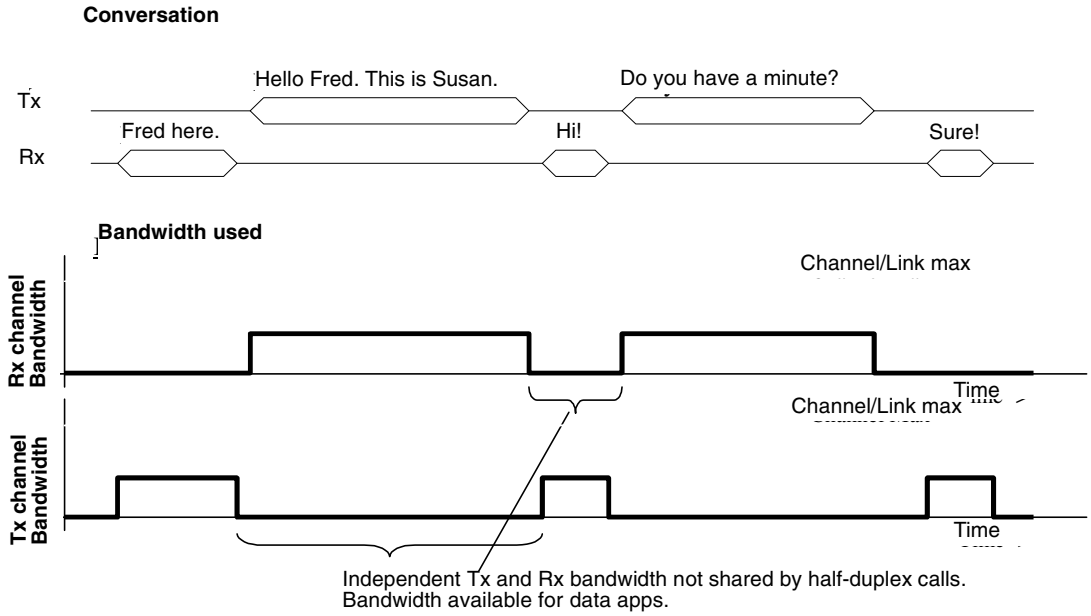
Figure 51 One Call on a Full Duplex Link Without Silence compression



When silence compression is enabled, voice packets are only sent when a speaker is talking. When a voice is being transmitted, it uses the full rate transmission rate. Since the sender and receiver do not share the same channel, the peak bandwidth requirement per channel is still equal to the full transmission rate. Figure 52 on page 107 below shows the peak bandwidth requirements for one call on a full-duplex link with silence compression enabled.

The spare bandwidth made available by silence compression is used for lower priority data applications that can tolerate increased delay and jitter.

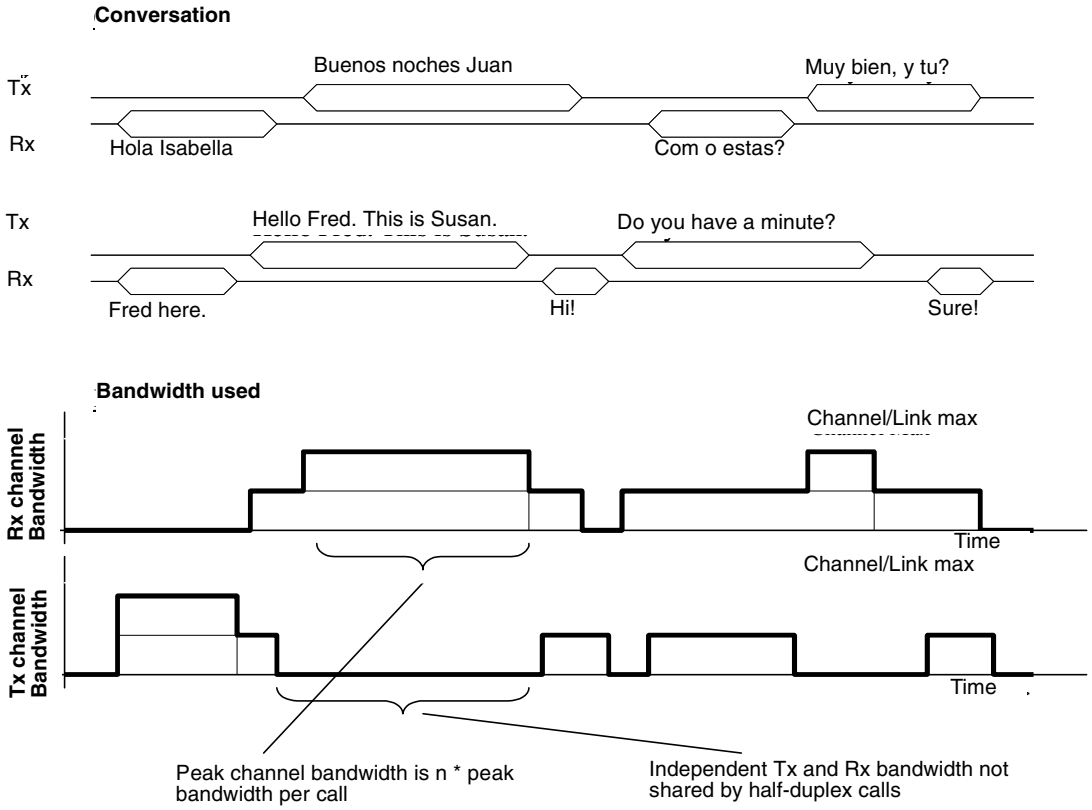
Figure 52 One Call on a Full Duplex Link With Silence compression



When several calls are made over a full duplex link, all calls share the same transmit path and they share the same receive path. Since the calls are independent, the peak bandwidth must account for the possibility that all speakers at one end of the link may talk at the same time. Therefore the peak bandwidth for n calls is n * the full transmission rate. Figure 2.6 below shows the peak bandwidth requirements for two calls on a full duplex link with silence compression. Note that the peak bandwidth is twice the full transmission rate even though the average bandwidth is considerably less.

The spare bandwidth made available by silence compression is available for lower priority data applications that can tolerate increased delay and jitter.

Figure 53 Two Calls on a Full Duplex Link With Silence compression



Comfort Noise

To provide a more natural sound during periods of silence, comfort noise is added at the destination gateway when silence compression is active. The source gateway sends information packets to the destination gateway informing it that silence compression is active and describing the background comfort noise to insert. The source gateway only sends the information packets when it detects a significant change in background noise.

Appendix C
Network Performance Utilities

There are two common network utilities, **Ping** and **Traceroute**. These utilities provide a method to measure quality of service parameters. Other utilities used also find more information about VoIP Gateway network performance.

Note: Because data network conditions can vary at different times, collect performance data over at least a 24 hour time period.

Ping

Ping (Packet InterNet Groper) sends an ICMP (Internet Control Message Protocol) echo request message to a host. It also expects an ICMP echo reply, which allows for the measurement of a round trip time to a selected host. By sending repeated ICMP echo request messages, percent packet loss for a route can be measured.

Traceroute

Traceroute uses the IP TTL (time-to-live) field to determine router hops to a specific IP address. A router must not forward an IP packet with a TTL field of 0 or 1. Instead, a router discards the packet and returns to the originating IP address an ICMP “time exceeded” message.

Traceroute sends an IP datagram with a TTL of 1 to the selected destination host. The first router to handle the datagram sends back a “time exceeded” message. This message identifies the first router on the route. Then Traceroute transmits a datagram with a TTL of 2.

Following, the second router on the route returns a “time exceeded” message until all hops are identified. The Traceroute IP datagram has a UDP Port number not likely to be in use at the destination (normally > 30,000). The destination returns a “port unreachable” ICMP packet. The destination host is identified.

`Traceroute` is used to measure round trip times to all hops along a route, identifying bottlenecks in the network.

Sniffer

Sniffer is not provided with the Business Communications Manager, but it is a useful tool for diagnosing network functionality. It provides origin, destination, and header information of all packets on the data network.

Appendix D
Interoperability

Business Communications Manager 2.5 IP Telephony adheres with the ITU-T H.323v2 standards, and is compatible with any H.323v1 or H.323v2 endpoints. Such endpoints include the Nortel Networks M1-ITG and Microsoft NetMeeting. As well, the Business Communications Manager is backward compatible, and interoperates with the Nortel Networks i2004 telephone and i2050 Software Phone, and with the Symbol NetVision IP Phones. Table 14 summarizes this information:

Table 14 Business Communications Manager 2.5 Product Interoperability Summary

Vendor	Product	Version
Nortel Networks	Business Communications Manager	2.5/2.0
Nortel Networks	i2004	3002B20 (or greater)
Nortel Networks	i2050	1.0.x
Nortel Networks	M1-ITG	ITG2.xx/1.xx
Microsoft	NetMeeting	3.0
Symbol	NetVision Phone (NVP)	03.50-12/01.00-24 (or greater)

Business Communications Manager IP Telephony also interoperates with any H.323v1 or H.323v2 compliant gateway that conforms to the specifications in the following tables.

Table 15 Engineering specifications

Capacity	1 to 8 ports
Voice compression	G.723.1 MP-MLQ, 6.3 kbit/s or ACELP, 5.3 kbit/s G.729 CS-ACELP, 8 kbit/s (supports plain, Annex A and Annex B) G.711 PCM, 64 kbit/s u/A-law
Silence compression	G.723.1 Annex A G.729 Annex B
Echo cancellation	48 ms tail delay
In-band signalling	DTMF (TIA 464B) Call progress
Speech path setup methods	Call Initiator: • H.323 slowStart Call Terminator: • H.323 slowStart • H.323v2 fastStart
End-to-end DTMF signaling	digits 0-9, # and *, fixed duration tones only

Table 16 Supported voice payload sizes

Codec	Receive/transmit to M1-ITG	Receive/transmit to others
G.711	Highest supported by both ends, up to 30 ms in 10 ms increments.	20 ms
G.723.1	30 ms	30 ms
G.729	Highest supported by both ends, up to 30 ms in 10 ms increments.	20 ms

Speech Path Setup Methods

Business Communications Manager 2.5 currently only initiates calls using H.323 slowStart methods. The Business Communications Manager will, however, accept and set up calls that have been initiated by another endpoint using H.323v2 fastStart methods, as well as H.323 slowStart methods.

Note that when using Symbol phones with Business Communications Manager 2.5, the Symbol phones will have to be configured to use H.323 slowStart only due to interoperability issues with fastStart between the Symbol telephones and the Business Communications Manager.

Media Path Redirection

Media path redirection occurs after a call has been established, when an attempt is made to transfer to or conference in another phone. Business Communications Manager 2.5 does not support codec re-negotiation upon media path redirection.

To ensure that call transfers, and conference works correctly, the following rules must be followed:

- The first preferred codec for VoIP Trunks must be the same on all Business Communications Managers. (See "Configuring codecs" on page 54). If this codec is G.729, or G.723, the Silence Suppression option must be the same on all Business Communications Managers involved.
- If interworking with a Meridian 1-ITG , the profile on the Internet Telephony Gateway (ITG) must be set to have the same first preferred codec as on the Business Communications Manager, the Voice Activity Detection (VAD) option must be set to the same value as the Silence Suppression on the Business Communications Manager and the ITG payload size must be set to 30 ms.
- Symbol telephones must be configured to use the same codec as the preferred codec on Business Communications Managers in the system.

If these rules are not adhered to, simple calls will still go through, but some transfer scenarios will fail.

Gatekeeper

The Business Communications Manager is designed to interoperate with any H.323v2 gatekeeper, with the Business Communications Manager supporting both Direct (GatekeeperResolved) and Routed (GatekeeperRouted) call signalling in this mode of operation. Note that if the call signalling method is changed, the Business Communications Manager must be restarted before it functions properly.

Asymmetrical Media Channel Negotiation

By default, the Business Communications Manager IP Telephony gateway supports the G.729 codec family, G.723.1, G.711 µ-law and G.711 A-law audio media encoding. Because NetMeeting does not support the H.323 fastStart call setup method, NetMeeting can choose a different media type for its receive and transmit channels. However, Business Communications Manager IP Telephony gateway does not support calls with different media types for the receive and transmit channels and immediately hangs up a call taken with asymmetric audio channels. In this case, the party on the Business Communications Manager switch hears a treatment from the switch (normally a reorder tone). The party on the NetMeeting client losses connection.

To solve this problem, in NetMeeting, under the **Tools**, **Options**, **Audio**, **Advanced**, check **Manually configure compression settings**, and ensure that the media types are in the same order as shown in the Business Communications Manager media parameters table. Table 17 on page 113 lists the names used by the Business Communications Manager local gateway table and the matching names in NetMeeting.

Table 17 Name comparison

Business Communications Manager media parameters table	MS NetMeeting
G.723.1 6.3 Kbit/s	MS G.723 6400 bit/s
G.723.1 5.3 Kbit/s	MS G.723 5333 bit/s
G.711 µ-law	CCITT µ-law
G.711 A-law	CCITT A-law

No feedback busy station

The Business Communications Manager VoIP gateway provides call progress tones in-band to the user. If a a busy station is contacted through the gateway, the gateway plays a busy tone to the user. However, as NetMeeting does not support fastStart, no speech path is opened to the user before the call connects. Because of this, the user on the NetMeeting station does not hear a busy signal from the gateway.

Symbol Telephones

The Business Communications Manager currently can only receive slowStart calls from a Symbol phone. Since the Symbol phones default to use H.323v2 fastStart, they must be changed to use slowStart. There are two methods that may be used to do this:

1. Manually edit the files created by NetVision Phone Administrator (NVPA) program. Add a configuration parameter to set the phones to use slowStart methods.
2. Log into the phone as a privileged user and set the call setup mode to slow start. See the Symbol documentation for more detailed information about this process.

In order to make calls between Symbol telephones and Business Communications Manager 2.5, each must be configured to have at least one common codec. The following codecs are supported by the Symbol telephones.

- G.711 u-law
- G.711 A-law
- G.729 Annex A and Annex B

Appendix E
Quality of Service

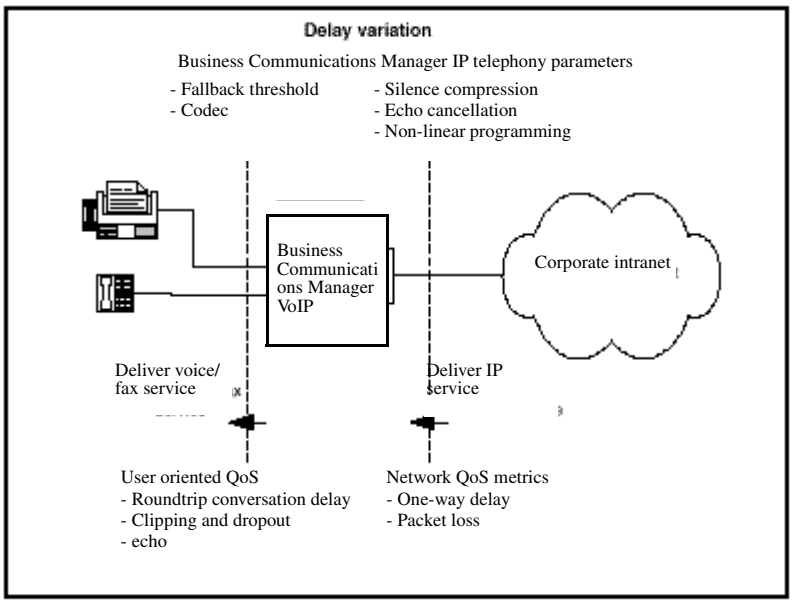
Setting QoS

The users of corporate voice and data services expect these services to meet a level of quality of service (QoS). This, in turn, affects network design. The purpose of planning is to design and allocate enough resources in the network to meet user needs. QoS metrics or parameters help in meeting the needs required by the user of the service.

There are two interfaces that must be considered:

- IP telephony interfaces with the end users: voice services made available need to meet user QoS objectives.
- The gateways interface with the intranet: the service provided by the intranet is “best-effort delivery of IP packets,” not guaranteed QoS for real-time voice transport. IP telephony translates the QoS objectives set by the end users into IP adjusted QoS objectives. The guidelines call these objectives the intranet QoS objectives.

Figure 54 Relationship between users and services



The IP gateway can monitor the QoS of the Intranet. In this mode, two parameters, the receive fallback threshold and the transmit fallback threshold control the minimum QoS level of the intranet. Fallback thresholds are set on pair-per-site basis.

The QoS level is aligned for user QoS metrics to provide an acceptable Mean Opinion Score (MOS) level. The administrator can adjust the fallback thresholds to provide acceptable service to the users.

Table 18 Quality of voice service

MOS Range	Qualitative Scale
4.86 to 5.00	Excellent
3.00 to 4.85	Good
2.00 to 2.99	Fair
1.00 to 1.99	Poor

The settings in Table 18 on page 116 indicate the quality of voice service. IP telephony periodically calculates the prevailing QoS level per site pair based on the measurement of the following:

- one-way delay
- packet loss
- codec

When the QoS level of any remote gateway is below the fallback threshold, all new calls are routed over the standard circuit-switched network if fallback is enabled.

The computation is taken from the ITU-T G.107 Transmission Rating Model.

Measuring Intranet QoS

Measure the end-to-end delay and error characteristics of the current state of the intranet. These measurements help to set accurate QoS needs when using the corporate intranet to carry voice services.

Measuring end-to-end network delay

The basic tool used in IP networks to get delay measurements is the Ping program. Ping takes a delay sample by sending a series of packets to a specified IP address and then return to the originating IP address. Ping then displays statistics for the packets. High packet times can indicate network congestion. If the packets time out, then the remote device is unreachable.

The round trip time (rtt) is indicated by the time field

So that the delay sample results match what the gateway experiences, both the Ping host and target must be on a functioning LAN segment on the intranet.

Set the size of the Ping probe packets to 60 bytes to approximate the size of probe packets sent by IP telephony. This determines if new calls need to fall back on the circuit-switched voice facilities.

Notice from the Ping output the difference of rtt. The repeated sampling of rtt allows you to receive a delay characteristic of the intranet. To get a delay distribution, include the Ping tool in a script which controls the frequency of the Ping probes, which timestamps and stores the samples in a raw data file.

The file can be analyzed by the administrator using spreadsheets and other statistics packages. The installer can check if the intranet network management software has any delay measurement modules which can cause a delay-distribution measurement for specific site pairs.

Delay characteristics vary depending on the site pair and the time of day. The evaluation of the intranet includes taking delay measurements for each site pair. If there are important changes of traffic in the intranet, include some Ping samples during the peak hour. For a more complete evaluation of the intranet delay characteristics, get Ping measurements over a period of at least a week.

Measuring end-to-end packet loss

The `Ping` program also reports if the packet made its round trip correctly. Use the same `Ping` host setup to measure end-to-end errors. Use the same packet size.

Sampling error rate, require taking multiple `Ping` samples (at least 30). An accurate error distribution requires data collection over a greater period of time. The error rate statistic from multiple `Ping` samples is the packet loss rate.

Recording routes

As part of the network evaluation, record routing information for all source destination pairs. Use the Traceroute tool to record routing information. A sample of the output of the Traceroute tool follows:

```
C:\WINDOWS>tracert 10.10.10.15

Tracing route to 10.10.10.15 over a maximum of 30 hops:

1 3 ms 1 ms <10 ms tftzraf1.ca.nortel.com [10.10.10.1]
2 1 ms 1 ms 1 ms 10.10.10.57
3 7 ms 2 ms 3 ms tcarrbf0.ca.nortel.com [10.10.10.2]
4 8 ms 7 ms 5 ms bcarha56.ca.nortel.com [10.10.10.15]

Trace complete.
```

The Traceroute program checks if routing in the intranet is symmetric for each source destination pairs. Also, the Traceroute program identifies the intranet links used to carry voice traffic. For example, if Traceroute of four site pairs gets the results shown in Table 19 on page 117, you can calculate the load of voice traffic per link.

Table 19 Site pairs and routes

Site pair	Intranet route
Santa Clara/Richardson	R1-R4-R5-R6
Santa Clara/Ottawa	R1-R2
Santa Clara/Tokyo	R1-R4-R5-R7
Richardson/Ottawa	R2-R3-R5-R6

Table 20 Computed load of voice traffic per link

Links	Traffic from
R1-R4	Santa Clara/Richardson
R4-R5	Santa Clara/Richardson Santa Clara/Tokyo
R5-R6	Santa Clara/Richardson Richardson/Ottawa
R1-R2	Santa Clara/Ottawa
R1-R4	Santa Clara/Tokyo
R5-R7	Santa Clara/Tokyo
R2-R3	Richardson/Ottawa
R3-R5	Richardson/Ottawa

Adjusting ping measurements

The Ping statistics are based on round-trip measurements. While the QoS metrics in the Transmission Rating model are one-way. To make the comparison compatible, the delay and packet error `Ping` statistics are halved.

Adjustment for processing

The `Ping` measurements are taken from `Ping` host to `Ping` host. The Transmission Rating QoS metrics are from end user to end user, and include components outside the intranet. The `Ping` statistics for delay needs additional adjustments by adding 140 ms to explain the processing and jitter buffer delay of the gateways.

No adjustments are required for error rates.

If the intranet measurement barely meets the round trip QoS objectives, the one-way QoS is not met in one of the directions of flow. This state can be true when the flow is on a symmetric route caused by the asymmetric behavior of the data processing services.

Late packets

Packets that arrive outside of the window allowed by the jitter buffer are discarded. To determine which `Ping` samples to ignore, calculate the average one-way delay based on all the samples. Add 300 ms to that amount. This amount is the maximum delay. All samples that exceed this one-way delay maximum are considered late and are removed from the sample. Calculate the percentage of late packets, and add that percentage to the packet loss statistics.

Measurement procedure

The following procedure is an example of how to get delay and error statistics for a specific site pair during peak hours.

Program a script to run the Ping program during intranet's peak hours, repeatedly sending a series of 50 Ping requests. Each Ping request generates a summary of packet loss, with a granularity of 2%, and for each successful probe that made its round-trip, that many *rtt* samples.

For a strong network there must be at least 3000 delay samples and 60 packet loss samples. Have the raw output of the `Ping` results stored in a file. Determine the average and standard deviation of *one-way delay* and *packet loss*.

Repeat this for each site pair. At the end of the measurements, the results are as shown in Table 21 on page 119.

Table 21 Delay and error statistics

Destination pair	Measured one-way delay (ms)		Measured packet loss (%)		Expected QoS level	
	Mean	Mean+σ	Mean	Mean+σ	Mean	Mean+σ
Santa Clara /Richardson	171	179	2	2.3	Good	Good
Santa Clara /Ottawa						
Santa Clara /Tokyo						
Richardson/ Ottawa						
Richardson/Tokyo						
Ottawa/Tokyo						

Other measurement considerations

The Ping statistics described above measure the intranet before IP telephony installation. The measurement does not take into consideration the expected load provided by the IP telephony users.

If the intranet capacity is tight and the IP telephony traffic important, the installer or administrator must consider making intranet measurements under load. Apply load using traffic generator tools; the amount of load must match the IP telephony offered traffic estimated in the Business Communications Manager VoIP Gateway Bandwidth requirements.

Decision: does the intranet meet IP telephony QoS needs?

The end of the measurement and analysis is a good indicator of whether the corporate intranet can deliver acceptable voice and fax services. The Expected QoS level column in Table 21 on page 119 indicates to the installer or administrator the QoS level for each site pair with the data.

To provide voice and fax services over the intranet, keep the network within a Good or Excellent QoS level at the Mean+σ operating area. Fax services must not travel on routes that have Fair or Poor QoS levels.

If QoS levels of some or all routes fall short of being Good, evaluate options and costs for upgrading the intranet. The evaluation often requires a link upgrade, a topology change, or implementation of QoS in the network.

To maintain costs, you can accept a Fair QoS level for the time for a selected route. A calculated trade-off in quality requires the installer or administrator monitor the QoS level, reset needs with the end users, and respond to user feedback.

Implementing QoS in IP networks

Corporate intranets are developed to support data services. Accordingly, normal intranets are designed to support a set of QoS objectives dictated by these data services.

When an intranet takes on a real-time service, users of that service set additional QoS objectives in the intranet, Some of the targets can be less controlled compared with the targets set by current services, while other targets are more controlled. For intranets not exposed to real-time services in the past, but which but now need to deliver IP telephony traffic, QoS objectives for delay can set an additional design restriction on the intranet.

One method is to subject all intranet traffic to additional QoS restrictions, and design the network to the strictest QoS objectives. A exact plan to the design improves the quality of data services, although most applications cannot identify a reduction of, say, 50 ms in delay. Improvement of the network results in a network that is correctly planned for voice, but over planned for data services.

Another plan is to consider using QoS in the intranet. This provides a more cost-effective solution to engineering the intranet for non-homogenous traffic types.

Traffic mix

This section describes QoS works with the IP telephony, and what new intranet-wide results can occur.

Before putting into operation QoS in the network, determine the traffic mix of the network. QoS depends on the process and ability to determine traffic (by class) so as to provide different services.

With an intranet designed only to deliver IP telephony traffic, where all traffic flows are equal priority, there is no need to consider QoS. This network can have one class of traffic.

In most corporate environments, the intranet supports data and other services. When planning to provide voice services over the intranet the installer determine the following:

- Is there existing QoS? What kind? IP telephony traffic must take advantage of established mechanisms if possible.
- What is the traffic mix? If the IP telephony traffic is light compared to data traffic on the intranet, then IP QoS can work. If IP telephony traffic is heavy, data services can be affected if QoS is biased toward IP telephony traffic.

TCP traffic behavior

Most of corporate intranet traffic is TCP-based. Different from UDP, that has no flow control, TCP uses a sliding window flow control mechanism. Under this design, TCP increases its window size, increasing throughput, until congestion occurs. Congestion results in packet losses, and when that occurs the throughput decreases, and the whole cycle repeats.

When multiple TCP sessions flow over few congestion links in the intranet, the flow control algorithm can cause TCP sessions in the network to decrease at the same time, causing a periodic and synchronized surge and ebb in traffic flows. WAN links can appear to be overloaded at one time, and then followed by a period of under-utilization. There are two results:

- bad performance ofWAN links
- IP telephony traffic streams are unfairly affected

Business Communications Manager Router QoS Support

With a Business Communications Manager system, the VoIP gateway and the router are in the same box. The Business Communications Manager router performs QoS and priority queuing to support VoIP traffic. The router supports VoIP in the following two ways:

- In a DiffServ network, Business Communications Manager system acts as a DiffServ edge device and performs packet classification, prioritization, and marking. The router performs admission control for H.323 flows based on the WAN link bandwidth and utilization. When received, the WAN link marks the H.323 flows as Premium traffic and places the flows in the high priority queue.

Note: Differentiated Service (DiffServ) is a QoS framework standardized by the Internet Engineering Task Force (IETF).

- In a non-DiffServ or a legacy network, the router manages the WAN link to make sure Premium VoIP packets have high priority in both directions when crossing a slow WAN link.

Network Quality of Service

Business Communications Manager VoIP Gateway uses a method like the ITU-T Recommendation G.107, the E-Model, to determine the voice quality. This model evaluates the end-to-end network transmission performance and outputs a scalar rating “R” for the network transmission quality. The packet loss and latency of the end-to-end network determine “R”. The model correlates the network objective measure “R”, with the subjective QoS metric for voice quality, MOS or the Mean Opinion Score.

This model provides an effective traffic building process by activating the Fallback to Circuit-Switched Voice Facilities feature at call set up to avoid quality of service degradation. New calls fall back when the configured MOS values for all codecs are below the threshold.

The model is the reason for compression characteristics of the codecs. Each codec delivers a different MOS for the same network quality.

Network Monitoring

The VoIP Gateway network monitoring function measures the quality of service between the local and all remote gateways on a continuous basis. The network monitoring function exchanges UDP probe packets between all monitored gateways to collect the network statistics for each remote location. All the packets make a round trip from the Sender to Receiver and back to the Sender. From this information, you can calculate the latency and loss in the network for a distinct location.

Note 1: Quality of Service monitoring is supported only on Business Communications Manager, M1 with ITG card, and i20xx.

Note 2: The Quality of Service threshold is configurable per remote gateway.

Note 3: Fallback starts for all new originating calls if the QoS of any monitored gateway is below its threshold.

Note 4: The fallback decision is made only at the originating gateway using the QoS thresholds monitored at the originating gateway for the destination gateway.

VoIP Gateway allows for manual configuration of QoS thresholds, depending on the customer preference between cost and voice quality.

Quality of Service parameters

Quality of Service depends on end-to-end network performance and available bandwidth. A number of parameters determine the VoIP Gateway QoS over the data network. The VoIP Gateway monitoring function can take about three minutes to respond to marginal changes in the network condition.

Packet loss

Packet loss is the percentage of packets that do not arrive at their destination. Transmission equipment problems, and high delay and congestion can cause packet loss. In a voice conversation, gaps in the conversation represent packet losses. Some packet loss, less than 5%, can be acceptable without audible degradation in voice quality.

Packet delay

Packet delay is the period between when a packet leaves and when a packet arrives at the destination. The total packet delay time includes fixed and variable delay. Variable delay is the more manageable delay, while fixed delay depends on the network technology. The distinct network routing of packets are the cause of variable delays. To minimize packet delay and increase voice quality, the gateway must be as close as possible to the network backbone (WAN) with a minimum number of hops.

Delay variation (jitter)

The amount of variation in packet delay is otherwise known as delay variations, or jitter. Jitter affects the ability of the receiving gateway to assemble voice packets received at irregular intervals into a continuous voice stream.

Fallback to PSTN

If the measured Mean Opinion Score (MOS) for all codecs is below the configured threshold for any monitored gateway, the Fallback to PSTN activates. This feature reroutes calls to different trunks such as the Public Switched Telephone Network (PSTN) until the network QoS improves. When the QoS meets or exceeds the threshold, calls route over the IP network.

Fallback can be caused by any of the following reasons:

- bad network conditions
- the remote gateway is out of service
- no network connection
- not enough DSP resources available

The fallback feature can be in the Local Gateway Configuration. With the fallback feature disabled, calls move across the IP telephony trunks no matter what level of Quality of Service. The fallback feature is active only at call setup. A call in progress does not fall back if the quality degrades.

Calls fallback if there is no response from the destination, an incorrectly configured remote gateway table, or if there are not enough DSP resources available to handle the new call.

Glossary

backbone

A network's major transmission path, handling high-volume, high-density traffic.

bandwidth

A measure of information carrying capacity available for a transmission medium, shown in bits per second. The greater the bandwidth, the more information sent in a given amount of time.

bridge

LAN equipment providing interconnection between two networks using the same addressing structure. A bridge filters out packets that remain on one LAN and forwards packets for other LANs.

codec

Equipment or circuits that digitally code and decode voice signals

communications protocol

A set of agreed-upon communications formats and procedures between devices on a data communication network.

data communications

Processes and equipment used to transport signals from a data processing device at one location to a data processing device at another location.

enbloc

All dialed digits sent in a single expression. The system waits for all digits to be dialled before processing the call.

full-duplex transmission

Simultaneous two-way separate transmission in both directions.

G.711

A codec that delivers "toll quality" audio at 64 kbit/s. This codec is best for speech because it has small delay, and is very resilient to channel errors.

G.729

A codec that provides near toll quality at a low delay. Uses compression to 8 kbit/s (8:1 compression rate).

G.723.1

A codec that provides the greatest compression, 5.3 kbit/s or 6.3 kbit/s. Normally used for multimedia applications such as H.323 videoconferencing. Allows connectivity to Microsoft-based equipment.

H.323

The ITU standard for multimedia communications over an IP network. Enterprise Edge IP Telephony supports H.323.

Hub

Center of a star topology network or cabling system.

kbit/s

kilobits per second. Thousands of bits per second.

Latency

The amount of time it takes for a discrete event to occur.

Mbit/s

Megabits per second. Millions of bits per second.

Modem

Device that converts serial data from a transmitting terminal to an analog device for transmission over a telephone channel. Another modem converts the signal to serial digital Noise

Random electrical signals, generated by circuit components or by natural interruptions, that damage communications.

Packet

Group of bits transmitted as a complete package on a packet switched network.

Packet switched network

A telecommunications network based on packet switching technology. A link is busy for the duration of the packets.

Terminal

Device capable of sending or receiving data over a data communications channel.

Throughput

Indicator of data handling ability. Measures data processed as output by a computer, communications device, link, or system.

Topology

Logical or physical arrangement of nodes or stations.

Voice Compression

Method of reducing bandwidth by reducing the number of bits required to transmit voice.

Index

A

acronyms 15

C

changes to the intranet 102

checklist 27

codecs
- defined 23
- for IP sets 33

Conventions and symbols 14

D

Danger symbol 14

default gateway
- on IP sets 35

DHCP
- configuring 38
- on IP sets 35

Dialing plan 56

E

end-to-end network delay 116

end-to-end packet los s117

Engineering Specifications 111

F

Fallback 123

firmware
- downloading to IP sets 43

G

Gatekeeper
- defined 22

gatekeeper
- interoperability 113

H

H.323 devices
- NetMeeting
  - interoperability 111

hop count 100

I

inappropriate load splitting 102

Installation
- IP sets 31

Interoperability 111

IP telephones
- 3-port switch 34
- Before Installing 33
- codecs 33
  - modifying 40
  - viewing 36
- default gateway 35
- defined 19
- DHCP 35, 38
- ethernet connection 34
- firmware
  - downloading 43
- installing 31
- Invalid server address 36
- Jitter buffer 33
  - modifying 40
- New Set 36
- No ports left 36
- ports 35
- registering 31
- registration 32
- Registration disable d36
- Set IP
  - viewing 36
- set IP 35
- settings
  - modifying 40
- subnet mask 35
- Troubleshooting 36

IP Telephony
- Benefits 19
- concepts 23
- Introduction 19

IP telephony
- networks 20

IP Telephony network
- DHCP 38

IP telephony network
- checklist 27

J

jitter 123

Jitter buffer
defined 24
IP sets 33
jitter buffer size 101

L

link delay 100

M

M1-ITG
defined 22
Interoperatibility 111
Measuring Intranet QoS 116
Media path redirection 111

N

network devices
checklist 28
network loading 96
network measurements 102

P

Packet delay 122
packet errors 101
Packet los s122
Ping 109
ping 118
ports
IP set 35
prerequisites 27

Q

QoS 120
defined 24
QoS Monitor 77
Quality of Service Monitor 77

R

Registration
IP sets 32
Routing and hop count 100
routing instability 102

S

speech path setup methods 111
subnet mask
IP sets 35
Symbol
interoperability 111
Symbols 14

T

text conventions 14
tip 14
Troubleshooting
IP sets 36

V

VoIP trunks defined 19

W

Warning symbol 14